

FortiWLM

User Guide

8.3.3

2017



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet® and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Support

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the [local contact numbers](#), or through the Support portal at <https://support.fortinet.com/>

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

Fortinet Product License Agreement / EULA and Warranty Terms



To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware

Trademarks and Copyright Statement

Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names may also be trademarks, registered or otherwise, of Fortinet. All other product or company names may be trademarks of their respective owners. Copyright © 2015 Fortinet, Inc., All Rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

Product License Agreement

The parties to this agreement are you, the end customer, and either (i) where you have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you have purchased your Product outside of the Americas, Fortinet Singapore Private Limited (each referred to herein as "Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT IMMEDIATELY NOTIFY THE FORTINET LEGAL TEAM IN WRITING AT LEGAL@FORTINET.COM OF REQUESTED CHANGES TO THIS AGREEMENT.

1. License Grant.

This is a license, not a sales agreement, between you and Fortinet. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if a substantial portion of your business is to provide managed service provider services to your end-customers, you may use the Software embedded in FortiGate and supporting hardware appliances to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation, and solely on the Fortinet appliance, or, in the case of blades, CPUs or databases, on the single blade, CPU or database on which Fortinet installed the Software or, for stand-alone Software, solely on a single computer running a validly licensed copy of the operating system for which the Software was designed, or, in the case of blades, CPUs or databases, on a single blade, CPU or database. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs or databases are licensed on a per single blade, solely for one blade and not for multiple blades that may be installed in a chassis, per single CPU or per single database basis, as applicable. The Software is "in use" on any Fortinet appliances when it is loaded into temporary memory (i.e. RAM). You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

2. Limitation on Use.

You may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner; (c) except as provided in section 5, transfer assign or sublicense right to any other person or entity, or (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers.

3. Proprietary Rights.

All rights, title, interest, and all copyrights to the Software and any copy made thereof by you and to any Product remain with Fortinet. You acknowledge that no title to the intellectual property in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific license as expressly set forth in section 1 ("License Grant") above. You agree to keep confidential all Fortinet

confidential information and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

Except for evaluation and beta licenses or other licenses where the term of the license is limited per the evaluation/beta or other agreement or in the ordering documents, the term of the license is for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet. The provisions of this Agreement, other than the license granted in section 1 ("License Grant"), shall survive termination.

5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (i) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products, you are not authorized to sell Product(s) or Software, but, regardless, by selling Product(s) or Software, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receive a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way.

6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website, <https://support.fortinet.com>, or such other website as provided by Fortinet, or for which the warranty otherwise

starts according to Fortinet's policies. The warranty periods discussed below will start according to Fortinet's policies posted at <http://www.fortinet.com/aboutus/legal.html> or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products, for any spare parts not purchased directly from Fortinet by the end-user, for any accessories, or for any stand-alone software. Fortinet warrants that the hardware portion of the Products, including spare parts unless noted otherwise ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): a three hundred sixty-five (365) day limited warranty for the Hardware excluding spare parts, power supplies, and accessories (provided, solely with respect to FortiAP and Meru AP indoor Wi-Fi access point Hardware appliance products and FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series (for both excluding spare parts, power supplies, and accessories), the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date), and, for spare parts, power supplies, and accessories, solely a ninety (90) days limited warranty. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that the software as initially shipped with the Hardware Products will substantially conform to Fortinet's then current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by

Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term "functional specifications" means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCUSSED ABOVE DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTITOKEN WHICH HAS A 365 DAY WARRANTY FROM THE DATE OF SHIPMENT FROM FORTINET'S FACILITIES, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTIGATE-ONE AND VDOM SOFTWARE. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE. The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or

errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided “as-is” without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user’s use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet.

8. Governing Law.

Any disputes arising out of this Agreement or Fortinet’s limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet’s limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE.

10. Import / Export Requirements; FCPA Compliance.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see www.bis.doc.gov. Fortinet assumes no responsibility or liability for your failure to obtain any

necessary import and export approvals, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you represent that you understand, and you hereby agree to comply with, all requirements of the U.S. Foreign Corrupt Practices Act and all other applicable laws. For beta, testing, evaluation, donation or free Products and/or related services, you hereby agree, represent and warrant to Fortinet that (a) receipt of the Products and/or services comply with all policies and you have obtained all necessary approvals for such Products and/or services, (b) the Products and/or services are not provided in exchange for Fortinet maintaining current business or for new business opportunities, and (c) the Products and/or services are not being received for the benefit of, and are not being transferred to, any government entity, representative or affiliate.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agree-

ment to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

14. Privacy.

For information regarding Fortinet's collection, use and transfer of your personal information please read the Fortinet privacy policy on the Fortinet web site (<http://www.fortinet.com/aboutus/privacy.html>).

15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify a Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US \$25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. In order to receive the modified software modules, you must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may be obtained by contacting Fortinet's Legal Department at legal@fortinet.com.

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the

Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if

the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under

this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of

definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this

License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is

given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.

Table of Contents

Support.	2
Introducing FortiWLM Application Suite	25
Audience	25
Other Sources of Information	26
Related Publications	26
END USER LICENSE AGREEMENT.	26
Contact	26
Getting Started with FortiWLM Application Suite	27
Setting Up Services Appliance.	27
Browser Settings	28
Delete Caching	29
Port Number Settings	30
Configuring FortiWLM Settings.	30
Network Settings between Server and Browser.	30
Other Network Settings	31
Configuring Service Assurance Manager Settings	31
Configuring Spectrum Manager Settings	31
SAM Installation Checklist	32
Spectrum Manager Installation Checklist	34
Add a License	35
Server Backup	35

Monitoring Network	37
How is Global Data Compiled?	38
Data Values Used to Plot Trend Graphs	38
Global Dashboard	39
Network Summary	40
Trends	40
Statistics	41
Controllers	42
AP Group Summary	42
Trends	43
Statistics	44
Trend Dashboard	45
Throughput Trend Graph	46
Station Trend Graph	46
Online AP Trend Graph	47
Offline AP Trend Graph	47
Ongoing Calls Trend Graph	48
Phones Trend Graph	48
Critical Alarms Trend Graph	49
High Noise Radios Trend Graph	49
High Loss Radios Trend Graph	50
High Loss Stations Trend Graph	50
Low Signal Stations Trend Graph	51
Rogue APs Trend Graph	51
Long Term Trend	52

Throughput	53
Controllers	53
APs	54
Stations	54
Phone Calls	54
Phones	55
Rx/Tx	55
Alarms	56
Distribution Dashboard	57
Throughput Distribution Graph	57
Stations Distribution Graph	58
Online APs Distribution Graph	58
Offline APs Distribution Graph	58
Ongoing Calls Distribution Graph	58
Phones Distribution Graph	58
Critical Alarms Distribution Graph	59
High-Noise Radios Distribution Graph	59
High-Loss Radios Distribution Graph	59
High-Loss Stations Distribution Graph	59
Low-Signal Stations Distribution Graph	60
Rogue APs Distribution Graph	60
Service Control	60
Application Visibility	61
Device Dashboard	62
Controller Dashboard	62

AP Dashboard	63
Nplus1 Clusters	64
Nplus1 Clusters section	66
Recent 10 events for all Nplus1 Clusters	67
List of Nplus1 Clusters	67
Cluster Details	68
Status Bar	69
Fault Dashboard	70
Alarms	70
Modifying Alarm Definitions	72
Filter History Alarms	74
Events	76
Modifying Event Definitions	78
Filter Events	78
Storage Info	79
Events - Storage Configuration	79
History Alarms - Storage Configuration	80
Station Activity	81
Station Trend Dashboard	81
Charts	82
Station Information	83
802.11 Session	83
Station History	83
Station Activity Log	84
Station Activity Log	84

Tools	85
Search Functionality	85
Station Topology	90
Controllers	90
Access Points	91
Stations	93
FortiWLM Status Bar	94
Configuring FortiWLM	97
Profiles	97
Wireless Service Profiles	98
Add a Service Profile in FortiWLM	99
Cloning Wireless Profile	103
Complete the Registration of a Service Profile in FortiWLM	103
Verify if a Controller is using NM or a Controller Configuration	106
ESS Profile in FortiWLM	107
Security Profile in FortiWLM	113
RADIUS Profile	118
Remote RADIUS Server	119
Before you Begin	119
How It Works	120
About Relay AP	120
Hotspot 2.0 Profile in FortiWLM	126
VLAN Profile in FortiWLM	130
Modify the Existing VLAN Profile	133
Rogue AP Detection	134

VLAN POOL	137
Features	137
Creating a VLAN Pool	138
Time Based ESS Profile	138
Creating a Timer Profile	138
GRE Profile in FortiWLM	140
Modify the Existing GRE Profile	142
Ethernet Profiles	143
Captive Portal Profiles	144
Social Authentication Support in Captive Portal	144
Create Captive Portal Exemptions Profile	145
Configure Captive Portal Profile to use Fortinet Presence	145
Enable this captive portal profile in security and ESS profiles	147
Templates	148
AP Template	148
Creating and Applying an AP Template	149
Updating an AP Template	149
Add a Radio Profile	151
Update the Radio Profile	153
Add Connectivity Profile	154
Update the Connectivity Profile	154
APs Not In Sync With NMS Configuration or Mismatched APs	155
Service Control	156
Modifying Service Control Global Configuration	157
Adding or Removing Services	160
Configuring Locations	162

Creating User Groups	162
Defining Service Control Policies	163
AP Init Scripts	164
Port Profiles	166
Creating a Port Profile	167
Push the Port Profile	168
Controller Configuration	169
Backup Controller Configuration	169
Performing a Manual Backup	169
Scheduling Automatic Backups	171
Controller Configuration Difference	172
Importing a Controller Configuration	173
DHCP Configuration	175
Creating a DHCP Server	175
Mesh Profiles	178
MAC Filtering	179
Guest Users	182
QoS Rules	182
QoS and Firewall Rule	183
Beacon Services	185
Adding Beacon Services Profiles	186
Enabling Beacon Services Profiles	187
Applying Beacon Services Profiles to APs	187
Editing Beacon Services Profiles	188
Deleting Beacon Services Profile	188
Exporting Beacon Services Profiles	188

Importing Beacon Services Profiles	189
Auto Radio Resource Provisioning (ARRP)	190
Configuring ARRP	191
Push ARRP Profiles	192
Limitations	192
Device Fingerprinting	192
Application Visibility	195
DSCP Marking	197
Valid DSCP value strings	197
Bandwidth Throttling	198
Configuration	198
Blocked Statistics	199
Create a policy	199
View blocked Statistics	199
Roaming Across Controllers	199
Monitoring Network Inventory	203
Devices	203
Controller Inventory	203
Add Controllers to FortiWLM	203
Modify Controllers	205
Access Points Inventory	211
How AP Discovery Works	211
Switches	215
Groups	216
Controller Group Inventory	216

Add a Controller Group	217
Modify a Controller Group	218
Delete a Controller Group	218
AP Group Inventory	219
Dynamic AP group	220
Software Upgrades	223
Images	223
Current Upgrades	224
Upgrade History	227
. Delete	228
Scheduled Upgrade	228
Create an Upgrade Schedule	229
Configured Upgrade Schedules	229
Reschedule Upgrades	229
Upgrade Limitations	229
Visualization	231
Heat Maps	231
Throughput Heat Map	231
Loss Heat Map	232
Channel Utilization Heat Map	233
Number of Stations Heat Map	234
Signal Strength Heat Map	235
Map Management	237
Import a Map Image	238
Add a Campus, Building, and Floor to the Map	238

Add APs, Floor APs and Landmarks to Maps	239
Viewing Maps	239
Reporting and Notification in FortiWLM.	241
Defining and Running Reports in FortiWLM.	241
Create Reports	241
Basic Information	243
Scope	245
Device Selection.	246
Reporting Interval.	247
Recurrence.	248
Report Generation Options	248
Station Reports	249
Top Stations	252
Unique Stations	253
AP Reports	255
Inventory Reports	259
Network Health Reports	262
Service Reports	266
View Reports	269
Scheduled Reports	269
Station Groups	270
Add Station Group	271
Edit Station Group	271
Delete Station Group	271
User Preferences	271

Set Up Email Notification	271
Add a Notification Profile	272
Add a FortiWLM Notification Filter	272
Service Assurance Manager (SAM) Notification	275
Troubleshooting Notification	275
Administration	277
System Administration	277
Server Parameters	277
Supported Controller Versions	278
Import NMS Agent tab	279
Mail Servers	280
Set Up Email Notification	280
Create a User on Email	281
Configure a Mail Server for Notification	281
SNMP Configuration	282
.	282
MIB Tables	282
Download the MIB Tables for Management Applications	282
Configure SNMP Service on Forti WLM With the Web UI	283
Capacity Threshold for Radio	285
System Log View	286
Export Syslog to External Server	287
FortiWLM Maintenance	289
FortiWLM Diagnostics	293
User Administration	294

Users and Users Group	294
User Group Access Capabilities.	295
Adding a User Group	295
Adding New Users	297
Remote Administrators.	298
FortiWLM Licensing	299
License Recovery and Backup.	299
Licensing and Upgrade	299
License Details	301
Backup Administration	302
Automated Backup	302
Backup History	302
Restoring a Backup	303
Deleting a Backup	304
Preserve Backup on Remote Server	304
Cleaning up of unwanted data	305
Flash Backup and Restore with Snapshot	305
Create a Flash Backup on Disk with Snapshot	305
Limitations for Flash Backup	306
Restore a Snapshot	306
Snapshot Restore Example	307
Corrupted Flash Example.	307
Reboot a Services Appliance and Select a Partition	308
Storage.	309
Station Activity Log	309

Security Administration	311
Security Certificate	311
Generate CSR on the FortiWLM	311
Server Certificates	311
Trusted Root CA Certificates	312
Configuring VPN Connections	313
Configuring the VPN	313
View the VPN Controllers and Status	314
High Availability	314
Configuring High Availability	314
Setting up Primary Server	314
HA Authentication (Primary Server)	314
IP Address High Availability (Primary Server)	315
Setting up the Backup Server	315
HA Authentication (Backup Server)	315
IP Address High Availability (Backup Server)	315
Status	316
Disabling the HA Cluster	316
Service Assurance Manager	321
Configuring SAM	323
Baseline Testing	323
Design a Baseline	323
Add a Baseline	323
Scheduling Tests	333

Add a Scheduled Test	333
Modify a Test Criteria	345
Enable a Test	345
Infrastructure	346
SAM Clients	346
Add Security Permission for SAM Clients.	346
Edit Security Permission for SAM Clients	347
Delete Security Permission for SAM Clients.	347
Add Security Permissions for Captive Portal	348
Captive Portal Types	348
Edit Captive Portal Types.	349
Delete Captive Portal Types.	350
Captive Portal Users	350
Edit Captive Portal Users	351
Delete Captive Portal Users	351
Get MACs.	352
Monitoring SAM.	355
Dashboard	355
Global Dashboard.	355
Controller Dashboard	356
Trends	357
Results Trends	358
Header Section.	358
Trend Graphs Section	360
Failure Trends.	364

Header Section	365
Failure Trends Graphs Section	366
Matrix Section	368
Monitor Tests	368
View Test Results for a Controller	368
View a Test in Progress	369
View all the Completed Tests	369
Definitions of Test Results	370
Reporting and Notification in SAM	371
PCI Compliance	373
Notification	373
Add a Notification Filter in SAM	373
Edit Notification Filters	375
Delete Notification Filters	375
SAM Administration	377
Maintenance	377
Licensing in SAM	378
License Usage Summary	378
Apply License	379
Remove License	380
Getting Started Spectrum Manager	381
Sensors Setup	381
Add Sensors to FortiWLM	382
Add Sensors to Map Management	383

Wireless Intrusions Prevention System (WIPS)	385
Monitoring Spectrum Manager	387
Spectrum Manager Dashboard	387
Event Log	389
Interference Event Clustering	390
Spectrum Manager - Recording Log	391
Spectrum Manager - Channel Availability	394
Spectrum Manager - Channel Utilization	395
Spectrum Manager - Spectrogram	396
Spectrum Manager - Equalizer	396
Spectrum Manager - Persistence	397
Control Panels	399
Sensors Filter	399
Sensors Hierarchy	399
Group Information	400
Time Filter	401
Start Time	401
Stop Time	401
Advanced Filter	402
Interference and Notes	403
Display Settings	404
Event Log - Display Settings	404
Recording Log - Display Settings	405
Channel Availability - Display Settings	405
Channel Utilization - Display Settings	406

Spectrogram - Display Settings	407
Equalizer - Display Settings	408
Persistence - Display Settings	410
Sensors.	412
Software Sensors	412
Hardware Sensors	412
RF Interferer Classification.	413
Radio frequency characteristics for the interferer devices	414
Sensors	417
RF Interferer Detection.	417
Historical Spectrum dashboard Analysis	418
Event logs	418
Time-based Analysis	418
Appendix A - Virtual Edition.....	421
Install and Configure VMware.	421
Download vSphere Client	422
Login to the vSphere Client	422
Create Virtual FortiWLM using vSphere client	422
Create Virtual FortiWLM using .OVA file	423
Create Virtual FortiWLM using .vmx and .vmdk file	427
Troubleshooting FortiWLM-Virtual Edition	445

Support for KVM Virtualization	445
Support for Hyper-V Virtualization	453
Creating Virtual Disk.	461
Post Configuration Settings.	464
Deploying FortiWLM with VMWare ESXi 6.5	471
Supported Hardware Configuration	471
Downloading the Virtual Machine Package File.	471
Creating the Virtual Machine	471
Configuring the Virtual Machine	475
Starting the Virtual Machine	476
Expanding the Virtual Hard Disk	476
Appendix B - Troubleshooting FortiWLM	479
Appendix C - Migrating FortiWLM Data.	487
Appendix D - Resetting System and System Passwords..	491
Appendix E - Command Line Interface	493
Appendix E - REST API	539
Sample Code	539
Fetch Access Token using username and password	539
Fetch Access Token using Refresh Token	540
Fetching Alarms data using the get API	541
AP Groups	542
Syslog / Activities	543

Station	544
Station Log	544
Access Points.	545
Network Summary	546
Alarms	546
Controller AP Inventory	548
Controllers	549
ESS	550
Security	552
Wireless	553
OAuth	554
Appendix F - WLAN Security Sensors capability	555

1 Introducing FortiWLM Application Suite

The *FortiWLM Application Suite* is an intelligent management system that helps you to easily manage your wireless network. It shares a common administrator interface, making it easy to transition between the following applications:

- **FortiWLM (NM)**—is a web based application suite which manages controllers and access points mapped to the network to provide real-time data that enables centralized and remote monitoring of the network.
- **Service Assurance Manager (SAM)**—provides trouble-prevention capability that uses the FortiWLM FortiWLM infrastructure to perform end-to-end system tests, either on-demand or automatically at periodic configured intervals. SAM works by comparing a well-functioning network baseline metric to periodic tests. Once baseline network performance is established, any tests that deviate from the baseline can trigger automatic notification. Multiple tests can be configured with *Service Assurance Manager*.
- **Spectrum Manager (SM)**—is used to manage your network health. The SM uses a network of devoted sensors or one of the radios on non-dedicated Fortinet AP400 Access Points, to continually scan the environment for interferences. With Fortinet Spectrum Manager, you can identify sources of potential interference and present interferer data on graphical dashboards to deliver high bandwidth and control the wireless spectrum for high quality of service (QoS).
The software based sensors detects and classifies sources of wireless interference and pro-actively manages channel interference issues. The sources for potential interference in 2.4 GHz and 5 GHz spectrum is identified and graphically represented on the dashboard.

This guide assumes that you have completed the hardware set up described in the *Fortinet Services Appliance Guide* and *FortiWLM Application Suite Release Notes*.

Audience

This guide is intended for network administrators configuring and maintaining *Fortinet Services Appliance* such as the SA250, SA2000 or SA2000-VE. The *Fortinet Services Appliance* such as the SA250 or SA2000 will have *FortiWLM* pre-installed on it.



The SA2000-VE will not have NM pre-installed on it.

Other Sources of Information

Additional information is available in the following Fortinet publications and external references.

Related Publications

- *Forti WLM Online Help*
- *Forti WLM Release Notes*
- *Fortinet Services Appliance Installation Guide*

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at <https://support.fortinet.com/>

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

2 Getting Started with FortiWLM Application Suite

Setting up *FortiWLM Application Suite* for the first time involves:

1. Setting up the services appliance (For instructions on setting up SA250 or SA2000, see *Fortinet Services Appliance Installation Guide*. For instructions on setting up SA2000VE, see [“Appendix A - Virtual Edition” on page 421](#))
2. Setting up *FortiWLM* via CLI (see [“Setting Up Services Appliance” on page 27](#) and [“Port Number Settings” on page 30.](#))
3. Installing a valid *FortiWLM*, *SAM*, and *Spectrum Manager* licenses (see [“Add a License” on page 35.](#))
4. Configuring any controllers to be managed by the services appliance (see [“Add Controllers to FortiWLM” on page 203.](#))
5. Configuring server backup settings (see [“Server Backup” on page 35.](#))

Follow through the sections below to complete the initial installation and configuration of *FortiWLM*.

Setting Up Services Appliance

The *FortiWLM* unit must be physically connected as described in the *Fortinet Services Appliance Installation Guide*. You will need the following items for software configuration:

- Run the **setup** command through the command line interface to configure the services appliance.
 - List of IP addresses and passwords.
 - Supported browsers is as mentioned below:
 - Internet Explorer 9 and later version
 - Mozilla Firefox 27.0 and 28.0
 - Google Chrome, version 34.0.1847.118 m
 - Licensing will be required, but not needed at this time.
1. Run the **setup** command through the command line interface. The **setup** command lists the following parameters of the services appliance to be configured:

- host name
- admin password
- To configure networking, select the option **yes** to modify the network settings.



By default, the services appliance IP address is configured to DHCP.

- Select the option **yes** to configure the *DHCP* Addressing and option **no** to configure the *Static* Addressing. The following parameters of the services appliance must be configured for static addressing:
 - IP address
 - netmask
 - default gateway (IP)
 - DNS server
 - DNS domain
 - Time zone settings
 - Synchronize the time with the NTP (Network Time Protocol) server.
2. The system restarts.
 3. After the services appliance restarts, use the **show nms** command to see the *IP address*.
 4. Login to the WebUI using https: <IP address>. At the login prompt, enter a *User ID* and *Password*. By default, the *guest* and *admin* user IDs are preconfigured.
 5. Create a signed server certificate using the instructions in the *Security Administration of NM*. (See [“Generate CSR on the FortiWLM”](#) on page 311.)



Before performing set up, ensure you are running the latest version of the FortiWLM Application Suite. Contact Fortinet support for the latest version of FortiWLM Application Suite.

Browser Settings

Before you begin, ensure your browser is configured to work with *FortiWLM*. The following are the supported browsers:

- Internet Explorer 9 and later version
- Mozilla Firefox 27.0 and 28.0
- Google Chrome, version 34.0.1847.118 m

The following configurations are described in this chapter:

Delete Caching

The dashboard updates are frequently ignored while using *FortiWLM Application*. To receive the dashboard updates, ensure to turn off the caching for the following browsers:

Browser	Steps to delete caching
Windows Internet Explorer	<p>The following steps must be performed, to turn off caching in <i>Windows Internet Explorer</i>:</p> <ol style="list-style-type: none">1. Open the <i>Internet Explorer</i>, select <i>Tools > Internet Options</i>.2. In the <i>Internet Options</i> window, select the <i>General</i> tab.3. From the <i>Browsing History</i> section in the <i>General</i> tab, click the <i>Settings</i> button.4. On the <i>Temporary Internet Files and History Settings</i> window, select “<i>Every time I visit the webpage</i>” option.5. Click <i>OK</i>.
Mozilla Firefox	<p>The following steps must be performed, to turn off caching in <i>Firefox</i>:</p> <ol style="list-style-type: none">1. Open a <i>Firefox</i>. Click <i>Tools > Options</i>.2. Select the <i>Privacy</i> panel.3. In the <i>History</i> section, set <i>Firefox will: to Use custom settings for history</i>.4. Select the check box for <i>Clear history when Firefox closes</i>.5. Beside <i>Clear history when Firefox closes</i>, click the <i>Settings</i> button. The <i>Settings for Clearing History</i> window will open.6. On the <i>Settings for Clearing History</i> window, click the following items to be cleared:<ul style="list-style-type: none">• Browsing History• Download History• Cookies• Cache• Active Logins7. Click <i>OK</i>. <p>To stop <i>Firefox</i> from caching future data, select <i>ask me every time</i> from the <i>Keep Until:</i> parameter.</p>

Browser	Steps to delete caching
Google Chrome	<p>The following steps must be performed, to turn off caching in <i>Google Chrome</i>:</p> <ol style="list-style-type: none"> 1. Click the <i>Chrome menu</i> on the browser toolbar. 2. Select <i>Tools</i>. 3. Select <i>Clear browsing data</i>. 4. In the dialog that appears, select the check boxes for the types of information that you want to remove. 5. Use the menu at the top to select the amount of data that you want to delete. Select <i>the beginning of time</i> to delete everything. 6. Click <i>Clear browsing data</i>.

Port Number Settings

This section provides the details to *Network Configuration* required for,

- “[Configuring FortiWLM Settings](#)” on page 30,
- “[Configuring Service Assurance Manager Settings](#)” on page 31 and
- “[Configuring Spectrum Manager Settings](#)” on page 31

Configuring FortiWLM Settings

Ensure the following ports must be open between *Controllers and Services Appliance*:

- UDP Port 5000, bi-directional
- Any SSH port, bi-directional (default port used is 22)
- TCP/UDP port 1194 for VPN discovery between the controller and *NM* server

Network Settings between Server and Browser

- The following ports are open between Server and Browser:
 - Port 443 for https
 - Port 80 for http
- Connect to *FortiWLM* by pointing a browser to the *Hostname/IP* address of the *NM* server or by providing a *Common Name* also known as *Fully Qualified Domain name* (FQDN) that is obtained while generating CSR. (See “[Generate CSR on the FortiWLM](#)” on page 311.)
- Provide a login and password (admin/admin is default). Since the controllers are not added to the *FortiWLM*, the WebUI will not display any data.

Other Network Settings

Open SMTP Port 25.

Configuring Service Assurance Manager Settings

The following *Service Assurance Manager* port numbers must be enabled, if the hardware platform running *SAM Server* and *Controller /AP* is behind a firewall.

- UDP ports 9494, 9595, 9596, 9597 between APs and *SAM* server for *SAM* to work
- Along with the above UDP ports, enable 5000 + Max Controller ID (shown in the inventory of *FortiWLM*) for TCP/UDP test accordingly for Throughput tests to work.

Configuring Spectrum Manager Settings

Enable the following *Spectrum Manager* port numbers:

- TCP/38182 between Sensor (PSM3x or AP433is) and *FortiWLM* server.
- TCP/38183 between the Client device (a laptop) and *FortiWLM* server.
- TCP/843 between the Client device (a laptop) and *FortiWLM* server.

The TCP/843 port is a flash policy server port. It enables to transfer a small flash policy file on the startup of each flash application.

All the above mentioned ports are bi-directional.

SAM Installation Checklist

SI No.	Question	Action
1	Are the APs <i>enabled</i> online, in L3 mode? Check on the controllers.	Check by clicking, <i>Configure > Devices > APs</i> . Look at the column Connectivity Layer. Also check by typing the CLI command show ap
2	Are the required controllers listed in the <i>FortiWLM</i> inventory and online-active in the <i>Forti-WLM</i> ?	Check by clicking, <i>Inventory > Devices > Controllers</i> .
3	The Release Notes reveals the version of the <i>FortiWLM</i> and <i>System Director</i> that is required. Are the controllers running a SAM-Supported build of <i>System Director</i> ?	Check by clicking, <i>Inventory > Devices > Controllers</i> .
4	Have two APs within the range? Are the two APs served with testing ESSIDs? Are the user credentials configured for <i>Radius</i> and <i>Captive Portal</i> based profiles on <i>SAM</i> ?	Ensure all the APs are at a minimum signal strength of -70dbm Download ESS on servicing APs to ensure the connection of the <i>SAM</i> client. Configure the corresponding <i>User Name</i> and <i>Password</i> in <i>SAM</i> for ESS which are served by external authentication servers.
5	Is anything obstructing the APs and services appliance for UDP ports 9494, 9595, 9596,9597. This can be difficult to determine. The Ports 5000 to 5000+ max controller ID or port 5000 + controller ID for each controller in <i>FortiWLM</i> box must be enabled.	Cross verify the owners of all switches, routers, and firewalls between the boxes.
6	Is NAT disabled/enabled?	NAT is not supported.

SI No.	Question	Action
7	Check if ICMP is successful between AP and SAM server.	The ICMP must be enabled in your network (particularly between the path of Server and AP).

Spectrum Manager Installation Checklist

Sl. No.	Question	Action
1.	Are the needed controllers listed in the <i>FortiWLM</i> inventory and online-active in the <i>FortiWLM</i> ?	Check <i>NM</i> by clicking, Inventory > Devices > Controllers.
2.	Are sensors enabled online in L3 mode in the controllers?	Check <i>NM</i> by clicking, Spectrum Manager > Monitor > Dash-board > Sensor Filter > Sensor Hierarchy or Spectrum Manager > Monitor > Sensors You can also verify on the controller, using the sh ap command.
3.	Do you have at least one sensor on each controller to be tested?	Check the controller by using the CLI command show interfaces Dot11Radio where the <i>AP Mode</i> displays as scan spectrum for a sensor AP.
4.	Are the following port numbers enabled in the firewall? <ul style="list-style-type: none"> TCP/38182 between the <i>Sensors</i> and <i>FortiWLM</i> server. TCP/38183 between the Client device (a laptop) and <i>FortiWLM</i> server. TCP/843 between the Client device (a laptop) and <i>FortiWLM</i> server. 	The necessary rules must be configured in the firewall if there is a firewall between the <i>Spectrum Manager</i> and sensors.
5.	Is NAT disabled/enabled?	NAT is not supported.
6.	Check the controller time and the <i>FortiWLM</i> time to see if they match.	If both the times do not match, sync them manually using setup command from the controller as well as the E(z)RF server. Using the NTP server is also preferred.

Sl. No.	Question	Action
7.	If you want to use software sensors, check if they are configured in the controller.	Configure the software sensors by using the CLI command, SMMC1550(15)# configure terminal SMMC1550(15)(config)# interface Dot11Radio 1 1 SMMC1550(15)(config-if-802)# mode scan-spectrum
8.	Check if the <i>Spectrum Manager</i> license is uploaded in <i>NM</i> server.	You can add SM license in <i>NM</i> using the following path: FortiWLM > User Administration > License
9.	Check whether the AP433is sensor is powered by AT power source.	Check the controller using the CLI command, show ap ap-id (The ap-id is an integer)

Add a License

The services appliance box includes an *Entitlement Certificate* with a number that is needed to procure a license file. Locate the *Entitlement Certificate* and follow the instructions to configure your license:

1. Contact Fortinet support for your license.
2. When you receive an email with the license file, save the file to your local system.
3. Apply the *FortiWLM* license to your services appliance by following the below steps:
 - Select *Administration > User Administration > License*. In the *License* screen select the *Upload License* option and choose the license key file and click open.
 - Select *Upload* to upload the license key file. The file is uploaded and is displayed on the *License Details* section.



The *Upload* license file allows a single license file upload. Multiple license file upload in one upload operation/session is not permitted.

Server Backup

1. Configure the server, to automatically transfer the backup to a remote server. Refer *"Backup Administration"* on page 302.

2. The nms-server provides an option to backup the database. The backup database is stored on the server in a pre-defined location (*/data/backup/nms*). The server backup performed can be moved between different nms-servers.
3. To configure the parameters, Refer to the *[“FortiWLM Maintenance”](#)* on **page 289**.

3 Monitoring Network

The *Monitor Dashboard* provides a summary view of all WLAN statistics. The graphical representation of *Alarms*, *Controllers*, *Access Points*, *Stations*, and *Station by OS* type provides a glimpse of the wireless network, based on the current and historical data stored in the database. The aggregate global trend performance and the error rate for all controllers are recorded over a period of time.

Trend Dashboard: The trend for a short term period (48 Hours) is recorded in the trend dashboard and the trend for up to one year is recorded in the long term trend dashboard.

Fault Management: A historical data of the raised alarms and events are maintained in the fault dashboard, allowing you to take appropriate action to maintain service.

Station Activity Log: The station activity displays the performance trends for a specific station. An intuitive graphical display of the *throughput*, *signal strength*, *loss*, and *airtime utilization* trends are plotted for the selected station.

Station History: The station history can be viewed and exported in CSV format (comma separated values.) The station types are filtered either based on the station event type or by selecting the *controller*, *event severity*, *event Id*, and *MAC address*.

Search: A powerful and flexible search function, including partial keyword search and advanced event filtering is enabled.

The graphical charts provide at-a-glance system information to the following dashboards available towards the left panel of each page:

- [“Global Dashboard” on page 39](#)
- [“Device Dashboard” on page 62](#)
- [“Fault Dashboard” on page 70](#)
- [“Station Activity” on page 81](#)
- [“Tools” on page 85](#)

How is Global Data Compiled?

The APs send the aggregated client data to the controller. *FortiWLM* gathers the controller data every ten minutes and stores it in database. The data is fetched from the database, when you access a particular dashboard. Every ten minutes, the raw data is compiled into summary charts and those statistics are displayed on the *Global Information Dashboard*.

Data Values Used to Plot Trend Graphs

Every ten minutes, these values are stored in the *FortiWLM* databases.

Parameter Name	Description / Data Type	Value Stored	Trend Dashboard	Longterm Trend Dashboard
Stations	# of associated stations	peak	Yes	Yes
Phones	# of registered phones	peak	Yes	Yes
Phone Calls	# of calls	average	Yes	Yes
Throughput	aggregated throughput	average	Yes	Yes
Rx Bytes	total bytes received	sum	-	Yes
Tx Bytes	total bytes transmitted	sum	-	
Online Controllers	# of online controllers	minimum	-	Yes
Offline Controllers	# of offline controllers	peak	-	
Online APs	# of online APs	minimum	Yes	Yes
Offline APs	# of offline APs	peak	Yes	
Critical Alarms	# of critical alarms	peak	Yes	Yes
Major Alarms	# of major alarms	peak	-	
Minor Alarms	# of minor alarms	peak	-	

Parameter Name	Description / Data Type	Value Stored	Trend Dashboard	Longterm Trend Dashboard
High Noise Radios	# of radios with high noise	NA. Instantaneous at the specific point in time	Yes	-
High Loss Radios	# of radios with high loss	NA. Instantaneous at the specific point in time	Yes	-
High Loss Stations	# of stations with high loss	NA. Instantaneous at the specific point in time	Yes	-
Low Signal Stations	# of stations with low signal	NA. Instantaneous at the specific point in time	Yes	-
Rogue APs	# of wired and wireless rogue APs	NA. Instantaneous at the specific point in time	Yes	-

Global Dashboard

The *Global Dashboard* provides at-a-glance system information to the following dashboards available in the left panel of each page:

- [“Network Summary” on page 40](#)
- [“AP Group Summary” on page 42](#)
- [“Trend Dashboard” on page 45](#)
- [“Long Term Trend” on page 52](#)
- [“Distribution Dashboard” on page 57](#)
- [“Service Control” on page 60](#)

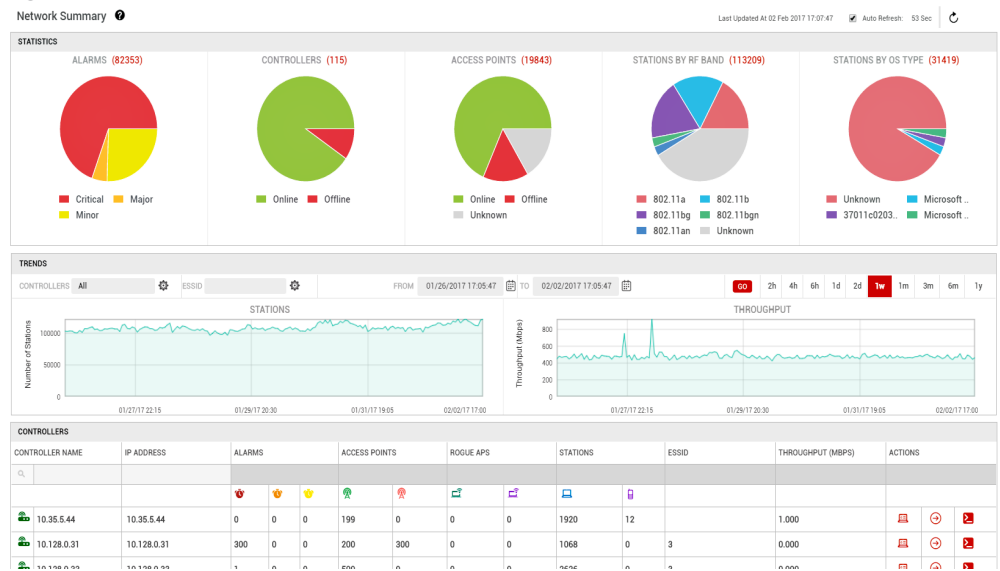
Network Summary

Monitor > Global Dashboard > Network Summary

The *Network Summary* dashboard provides a summary view of the WLAN statistics, including network wide wireless controller and access point performance distribution. It gathers data from all managed controllers and access points at specific intervals. The graphical representation of *Alarms*, *Controllers*, *Access Points*, *Stations*, and *Station by OS type* provides you a glimpse of the wireless network, based on the current and historical data stored in the data-base.

Figure 1 on page 40 illustrates the *Network Summary Dashboard* screen.

Figure 1: Network Summary Dashboard



The *Network Summary* dashboard provides data from *Trends*, *Statistics*, and *Controllers*.

Trends

Trends section of the *Network Summary* dashboard provides a graphical representation of the controller statistics which are under administrative scope of your access settings. The trends based on *Controllers* and *SSID* selection is monitored by selecting the trend duration for 2 hours, 4 hours, 6 hours, 1 day, 2 days, 1 week, 1 month, 6 months or 1 year. Either a single controller or all the controllers can be selected. The two types of Trends are described below:



- **Number of Stations:** This graph displays the aggregate number of wireless stations connected to the network.






- **Bandwidth Utilization (Mbps):** This graph displays the aggregate bandwidth utilization (in Mbps) across all controllers.

Statistics

Statistics section provides you the following five pie charts within the wireless network:

- **Alarms:** It provides you the total number of *critical*, *major*, and *minor* alarms.
 - The *critical* alarms are displayed in red color, *major* alarms in orange color and *minor* alarms in yellow color.
 - Hover the mouse pointer over a graph to view total alarms.
 - Left click on each of the sections to view a detailed summary of the alarm (displayed in a pop-up box.)
- **Controllers:** This pie chart provides the total number of *online* and *offline* controllers.
 - The *online* controllers are displayed in green color and *offline* controllers are displayed in red color.
 - Hover the mouse pointer over a graph to view total controllers.
 - Left click on each of the sections to view a detailed summary of the controller (displayed in a pop-up box.)
- **Access Points:** This pie chart provides the total number of *online*, *offline*, and *unknown* access points.
 - The *online* access points are displayed in green color, *offline* access points in red color and *unknown* access points in grey color.
 - Hover the mouse pointer over a graph to view total access points.
 - Left click on each of the sections to view a detailed summary of the access points (displayed in a pop-up box.)
- **Stations:** This pie chart provides the station classification based on the RF Type. It displays the total number of stations connected to a particular RF type.
 - Each station type is represented in a unique color. Hover the mouse pointer over a graph to view the total number of stations connected to a particular RF type.

Stations	Description	Color
802.11a	802.11a is a wireless standard that is implemented on 5GHz frequency range with a maximum data rate of 54Mbps.	
802.11b	802.11b is a wireless standard that is implemented on 2.4GHz frequency range with a maximum data rate of 11Mbps.	

Stations	Description	Color
802.11bg	802.11bg is a wireless standard that works on 2.4GHz frequency range with a maximum data rate of 54Mbps.	
802.11bgn	802.11bgn is a wireless standard that is implemented on 2.4GHz and frequency range with a maximum data rate of 600Mbps.	
802.11an	802.11an is a wireless standard that is implemented on 5GHz and frequency range with a maximum data rate of 600Mbps.	
802.11ac	802.11ac is a wireless standard that is implemented on 5GHz and frequency range with a maximum data rate of 1Gbps	
Unknown	Unknown state is displayed when the system is unable to find the RF band of the station.	

- Left click on each of the sections to view a detailed summary of the station (displayed in a pop-up box.)
- **Stations by OS Type:** This pie chart provides the station classification based on the operating systems type (OS type).
 - Each station is represented by a unique color.
 - Hover the mouse pointer over a graph to view total number of stations.
 - Left click on each of the OS type to view a detailed summary of the stations connected to the controller by different OS Type (displayed in a pop-up box.)

Controllers

Controller section provides a summary of the *online*, *offline*, and *unmanaged* controllers. It provides the status of *Alarms*, *Access Points*, *Stations*, *SSID*, and *Throughput* of the controller.

AP Group Summary

Monitor > Global Dashboard > AP Group Summary

An AP Group is a coherent group of APs belonging to the same controller or different controllers placed in distinctive geographic locations. The AP group may consist of APs with different hardware model or APs from controllers having different *System Director* versions. When an AP is added to a group, all the radios of the AP are also a part of this group. The *FortiWLM* provides the following operations at the AP Group level.

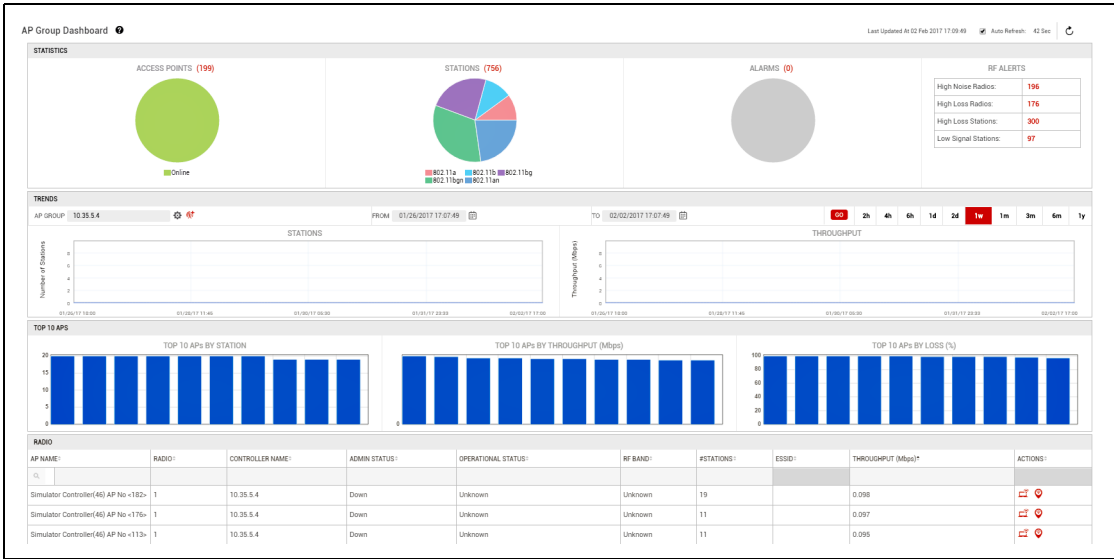
- Monitoring

- Service configuration
- Notification

The APs data within the selected *AP Group* is used to create *AP Group Dashboard*. The data is generated every 10 minutes on the server. The aggregation time or the *Auto Refresh* time is located towards the right side corner of the dashboard. All the links or pop-up from this page and status bar display the current data.

Figure 2 on page 43 illustrates the *AP Group Dashboard* screen.

Figure 2: *AP Group Dashboard*



The AP Group Summary dashboard provides data from *Trends*, *Statistics*, *Top 10 APs*, and *Radio*.

Trends

Trends section of the *AP Group* dashboard graphically represents the AP statistics that belong to a selected AP group which are under administrative scope of your access settings. You can monitor the AP group trends by selecting the trend duration for 2 hours, 4 hours, 6 hours, 1 day, 2 days, 1 week, 1 month, 6 months or 1 year. Single or all the AP Groups can be selected. AP groups can also be created by selecting the *create AP group* icon. Two types of trends are described below:




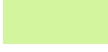


- **Number of Stations:** This graph displays a trend of aggregate number of stations connected to the APs within the selected AP group.


- **Bandwidth Utilization (Mbps):** This graph displays the aggregate bandwidth utilization (in Mbps) of the selected AP group.

Statistics

Statistics section of the AP group dashboard graphically represents the statistical data of the selected *AP Group*, *Stations*, and *Alarms* within the wireless network. The following are the three types of pie charts and RF Alerts:

- **Access Points:** This pie chart provides the total number of *online*, *offline*, and *unknown* access points.
 - The *online* access points are displayed in green color, *offline* access points in red color and *unknown* access points in grey color.
 - Hover the mouse pointer over a graph to view total number of access points.
 - Left click on each of the sections to view a detailed summary of the access points (displayed in a pop-up box.)
- **Stations:** This pie chart provides the station classification based on the RF Type. It displays the total number of stations connected to a particular RF type.
 - Each station type is represented in a unique color. Hover the mouse pointer over a graph to view the total number of stations connected to a particular RF type.

Stations	Description	Color
802.11a	802.11a is a wireless standard that is implemented on 5GHz frequency range with a maximum data rate of 54Mbps.	
802.11b	802.11b is a wireless standard that is implemented on 2.4GHz frequency range with a maximum data rate of 11Mbps.	
802.11bg	802.11bg is a wireless standard that works on 2.4GHZ frequency range with a maximum data rate of 54Mbps.	
802.11bgn	802.11bgn is a wireless standard that is implemented on 2.4GHz and frequency range with a maximum data rate of 600Mbps.	
802.11an	802.11an is a wireless standard that is implemented on 5GHz and frequency range with a maximum data rate of 600Mbps.	
802.11ac	802.11ac is a wireless standard that is implemented on 5GHz and frequency range with a maximum data rate of 1Gbps	

Stations	Description	Color
Unknown	Unknown state is displayed when the system is unable to find the RF band of the station.	

- Left click on each of the sections to view a detailed summary of the station (displayed in a pop-up box.)
- Alarms: This pie chart provides the total number of *critical*, *major*, and *minor* alarms.
 - The *critical* alarms are displayed in red color, *major* alarms in orange color and *minor* alarms in yellow color.
 - Hover the mouse pointer over a graph to view total number of the alarms raised.
 - Left click on each of the sections to view a detailed summary of the alarm (displayed in a pop-up box.)
- RF Alerts: The RF Alerts provides the
 - *High Noise Radios* experiencing high Noise (> -70 dBm),
 - *High Loss Radios* experiencing high loss (> 50%),
 - *High Loss Stations* experiencing high loss (> 50%), and
 - *Low Signal Stations* experiencing low signal (< -80 dBm).

Left click on each of the above sections to view a detailed summary of the RF Alert (displayed in a pop-up box.)

- Bar Charts: The *Bar Charts of APs by Stations*, *APs by Bandwidth Usage* and *APs by Loss* is displayed based on the top 10 APs.
- **Radio Status and State:** The *Radio Status and State* table displays the basic information and statistics of the radios. It provides *AP Name*, *Radio*, *Controller*, *Admin Status*, *Operational Status*, *RF Band*, *Stations*, *SSID*, *Throughput*, and *Actions of each AP within the wireless network*.

Trend Dashboard

Monitor > Global Dashboard > Trend Dashboard

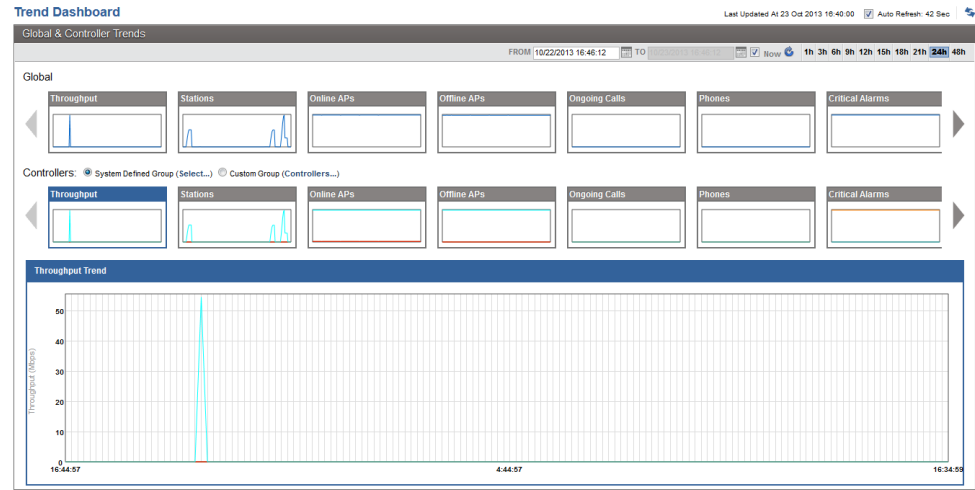
Trend Dashboard provides you the aggregate global trend performance and controller error rates over a period of time. *FortiWLM* collects statistics from a controller every ten minutes and stores it in the database. The Trend dashboard provides the data collected for a single controller or up to five controllers. The trends per controller can be edited by selecting the controllers from the *Custom Group* option on the Trend Dashboard.

The global trends and trends per controller are graphically represented in the *Trend Dashboard*. displays the *global trends* (all controllers) in the graphs on the top portion of the window and trends per controller on the lower portion of the window. Multiple lines are sometimes displayed in the lower set of charts due to multiple controller selection. The information about the

controller trend graph is plotted for past 1 to 48 hours by representing up to five controllers at a time. The time period can be modified from 1 to 48 hours by selecting the Trend Interval or by selecting the “From” and “To” duration of time.

Figure 3 on page 46 illustrates the *Trend Dashboard* screen.

Figure 3: *Trend Dashboard*



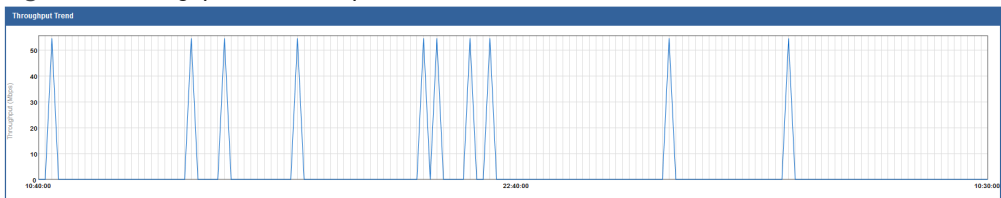
Throughput Trend Graph

Select the small *Throughput* graph to see a larger version displayed in the middle of the screen.

Figure 4 on page 46 illustrates the *Throughput Trend* graph.

The default *Throughput Trend* graph illustrates the throughput trend for the network (upper graph) and individual controllers (lower graph). The lower graphs are trends for selected controllers; the objective here is to compare relative performance of up to five controllers.

Figure 4: *Throughput Trend* Graph



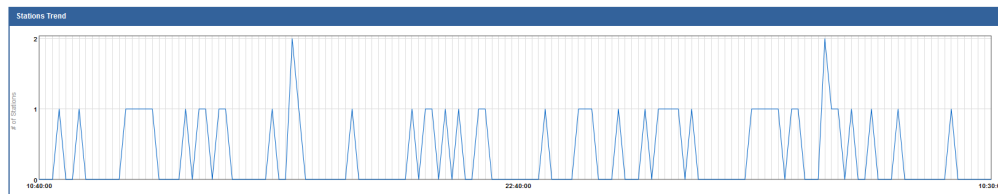
Station Trend Graph

Select the small *Stations* Graph to see a larger version displayed in the middle screen. By default, the *Throughput* graph is displayed which cannot be modified.

Figure 5 on page 47 illustrates the *Station Trend Graph*.

The lower graphs displays station trends for selected controllers; the *Station Trend Graph* showcases the number of stations on up to five controllers.

Figure 5: Station Trend Graph



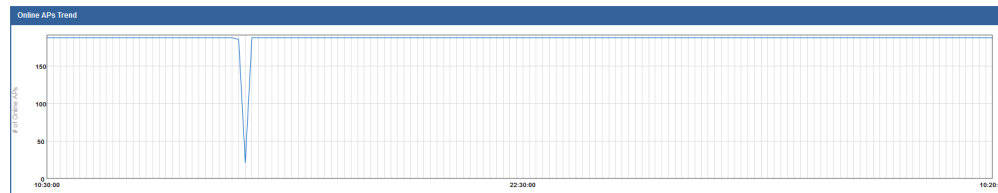
Online AP Trend Graph

Select the small *Online AP* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

Figure 6 on page 47 illustrates the *Online AP Trend Graph*.

The upper graph represents the number of online APs on all controllers currently managed by *FortiWLM* that are up and running. The lower graphs are *Online AP Trends* for selected controllers; the objective here is to compare the number of online APs for up to five controllers.

Figure 6: Online AP Trend Graph



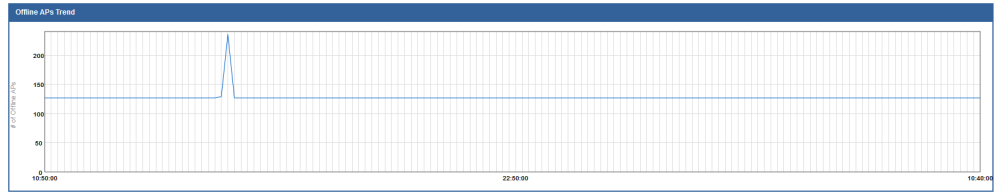
Offline AP Trend Graph

Select the small *Offline AP* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

Figure 7 on page 48 illustrates the *Offline AP Trend Graph*.

The upper graph represents the trend for APs on all controllers managed by *FortiWLM* that are not running. The lower graphs are *Offline AP Trends* for selected controllers; the objective here is to compare the number of offline APs on up to five controllers.

Figure 7: Offline AP Trend Graph



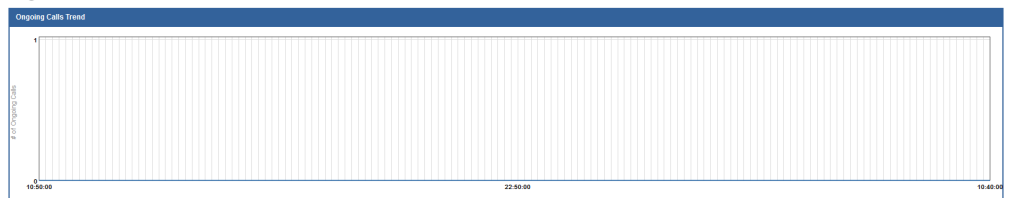
Ongoing Calls Trend Graph

Select the small *Ongoing Calls* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

Figure 8 on page 48 illustrates the *Ongoing Calls Trend Graph*.

For the upper graph, all ongoing calls are counted on every controller currently managed by *FortiWLM*. The lower *Ongoing Calls Trend* graph represents calls for up to five selected controllers; the objective here is to compare the number of ongoing calls on these controllers.

Figure 8: Ongoing Calls Trend Graph



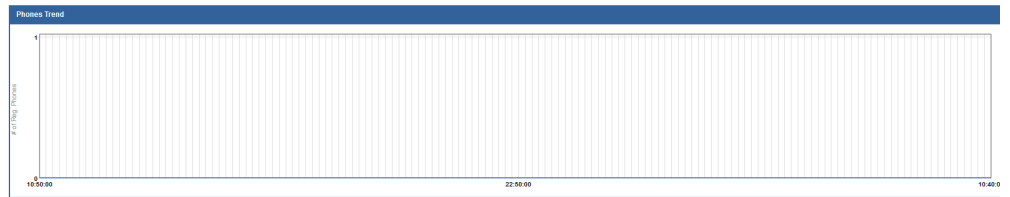
Phones Trend Graph

Select the small *Phones* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

Figure 9 on page 49 illustrates the *Phones Trend Graph*.

The phones associated to any of the APs or controllers managed by the *FortiWLM*. The upper graph shows the trend for all registered phones for all controllers. The lower *Phones Trend* graph represents phones for up to five selected controllers; the objective here is to compare the number of phones on these controllers.

Figure 9: Registered Phones Trend Graph



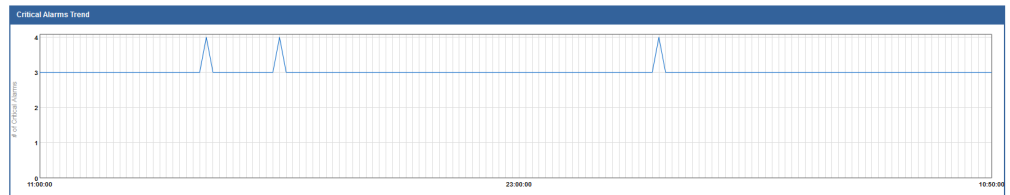
Critical Alarms Trend Graph

Select the small *Alarms* graph to see a larger version displayed in the middle screen. By default, the *Throughput* graph is displayed which cannot be modified.

Figure 10 on page 49 illustrates the *Critical Alarms Trend Graph*.

The upper graph shows the trend for all alarms on all controllers in a line chart. The lower *Critical Alarms Trend* graph represents alarms for up to five selected controllers; the objective here is to compare critical alarm count on these controllers. Typical examples of critical alarms are AP Down and Rogue AP Detected.

Figure 10: Critical Alarms Trend Graph



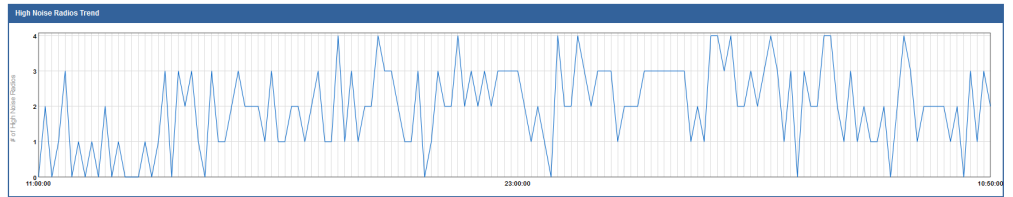
High Noise Radios Trend Graph

Select the small *High Noise Radios* graph to see a larger version displayed in the middle screen. By default, the *Throughput* graph is displayed which cannot be modified.

Figure 11 on page 50 illustrates the *High Noise Radios Trend Graph*.

The *High Noise Radio Trend* graph displays the aggregate number of radios experiencing noise greater than threshold (-70 dBm).

Figure 11: High Noise Radios Trend Graph



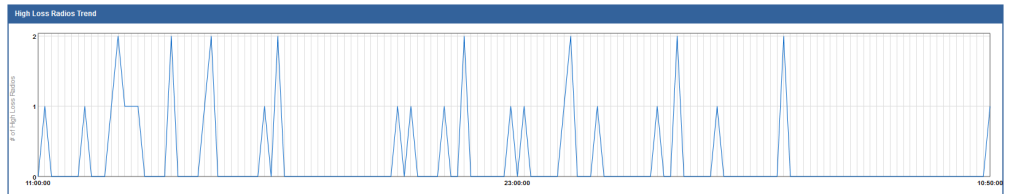
High Loss Radios Trend Graph

Select the small *High Loss Radios* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

[Figure 12 on page 50](#) illustrates the *High Loss Radios Trend Graph*.

The *High Loss Radios Trend* graph displays the aggregate number of radios experiencing loss greater than the threshold (50%). You cannot modify the threshold at this time.

Figure 12: High Loss Radios Trend Graph



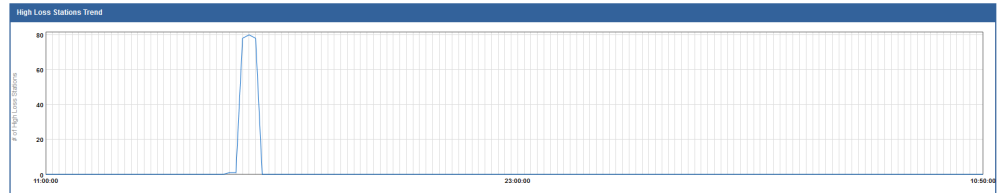
High Loss Stations Trend Graph

Select the small *High Loss Stations* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

[Figure 13 on page 51](#) illustrates the *High Loss Stations Trend Graph*.

The *High Loss Stations Trend* graph displays the aggregate number of high-loss stations for each three minute period. High loss is defined as 50%.

Figure 13: High Loss Stations Trend Graph



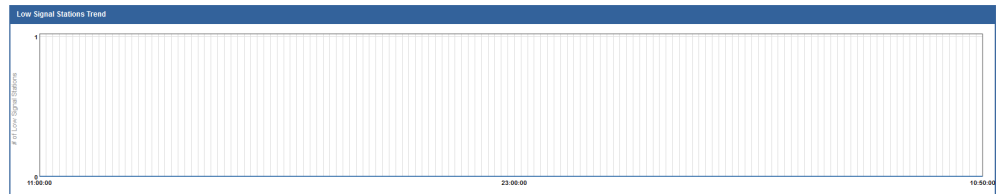
Low Signal Stations Trend Graph

Select the small *Low Signal Stations* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

Figure 14 on page 51 illustrates the *Low Signal Stations Trend Graph*.

The *Low Signal Stations Trend* graph displays the aggregate number of radios on all controllers that are experiencing loss greater than the threshold (50%). You cannot change thresholds at this time.

Figure 14: Low Signal Stations Trend Graph



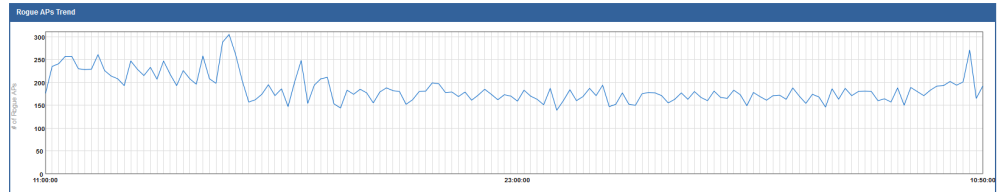
Rogue APs Trend Graph

Select the small *Rogue APs* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

Figure 15 on page 52 illustrates the *Rogue APs Trend Graph*.

The *Rogue AP Trend* graph represents the classification of controllers into ten groups based on number of rogue APs detected on each controller.

Figure 15: Rogue APs Trend Graph



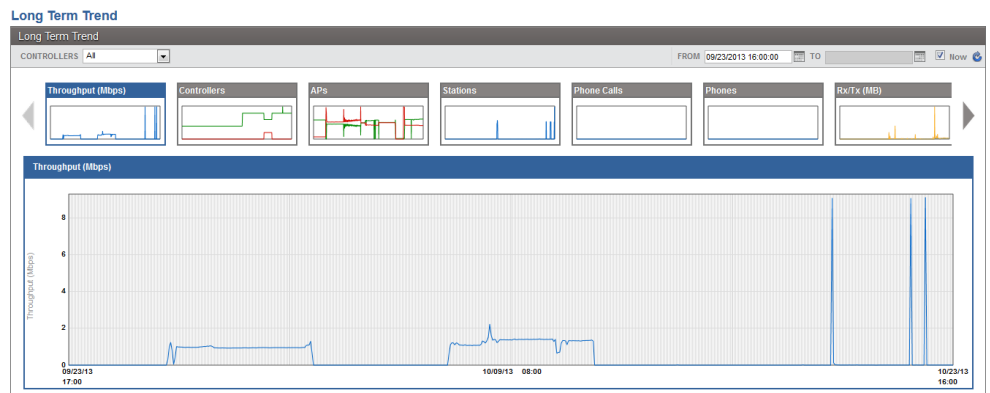
Long Term Trend

Monitor > Global Dashboard > Long Term Trend

The *FortiWLM* collects the statistical data from the controller for every ten minutes and provides an option to view the *Long Term Trend* for the predefined parameters. The *Long Term Trend* data is a graphical representation for the statistics gathered over the period of time.

[Figure 16 on page 52](#) illustrates the *Long Term Trend* screen.

Figure 16: Long Term Trend Dashboard



The *Long Term Trend Dashboard* displays the per-controller view or the aggregate-controller view (default view). The trend data for a maximum of one year and a minimum period of one hour for either all controllers or for one particular controller is displayed. The Long Term Trend data stored in the *FortiWLM* database cannot be modified. The *FortiWLM* summarizes the data in three predefined sample periods as follows:

- **Hourly:** If the time range to be graphed is 1 month or less than one month, the trend graph is displayed with hourly sample points. This is the default view.
- **8 Hours:** If the time range to be graphed is more than one month and less than 8 months, the trend graph is displayed with 8 hours sample points. The sampling time can also be configured on the *Maintenance* screen (*Administration > Maintenance > Statistics* section > *Long Term: 8 Hourly Data Aggregation Period Begins At (AM)*)

- **24 Hours:** If the time range to be graphed is more than 8 months and up to 1 year, the trend graph is displayed with 24 hours sample points.

The long-term trend graphs display up to 12 months of data for either the selected controller or all controllers available to the user group.

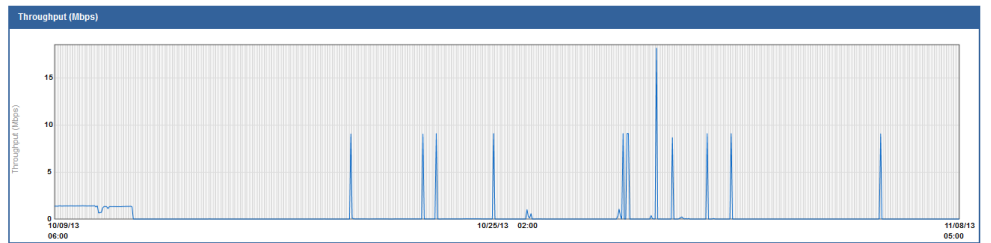
Throughput

The *Throughput* graph represents the total number of controllers' throughput aggregated.

Figure 17 on page 53 illustrates the *Throughput long term trend graph*.

Right click and select *Show Details* on the Throughput graph to view the details of Throughput.

Figure 17: *Throughput long term trend graph*

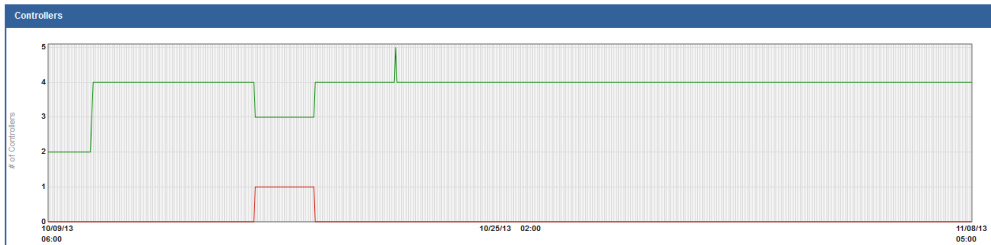


Controllers

The *Controllers* graph represents total number of polled controllers. Both *online* (green) and *offline* (red) controllers can be viewed.

Figure 18 on page 53 illustrates the *Controllers long term trend graph*.

Figure 18: *Controllers long term trend graph*



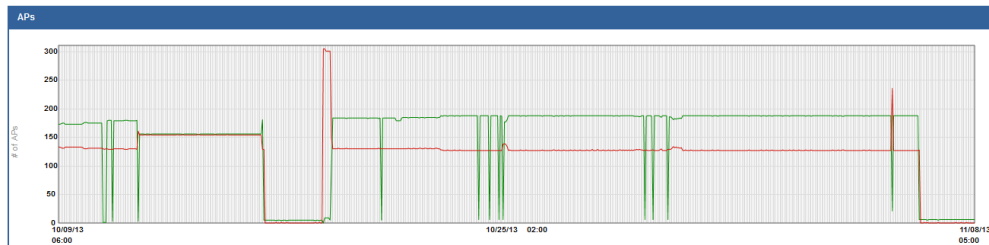
The number of managed controllers in the controllers graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of online and offline controllers.

APs

The *APs* graph represents the total number of APs present on the polled controllers. Both online (green) and offline (red) APs can be viewed.

Figure 19 on page 54 illustrates the *APs Long Term Trend* graph.

Figure 19: *APs long term trend graph*



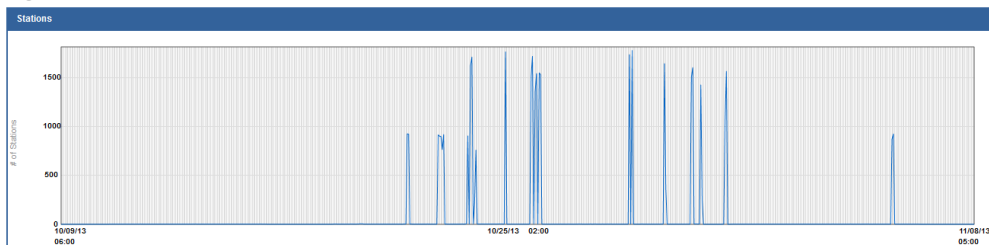
The number of APs present on the managed controllers in the *APs* graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the online and offline APs.

Stations

The *Stations* graph represents the total number of stations associated to *FortiWLM* controllers for the selected time period.

Figure 20 on page 54 illustrates the *Stations Long term trend* graph.

Figure 20: *Stations long term trend graph*



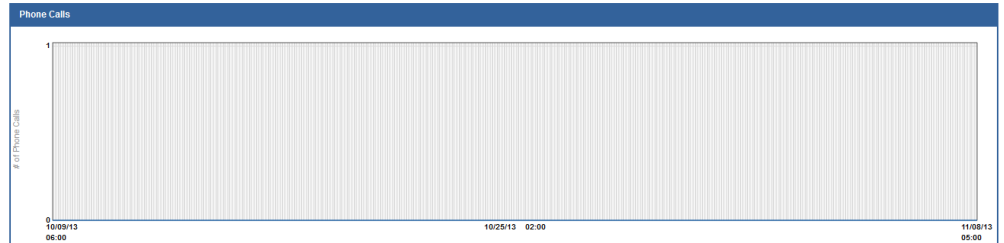
The number of stations in the *Stations* graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the stations associated.

Phone Calls

The *Phone Calls* graph represents the aggregate number of all the current wireless phone calls.

Figure 21 on page 55 illustrates the *Phone Calls long term trend* graph.

Figure 21: Phone Calls long term trend graph



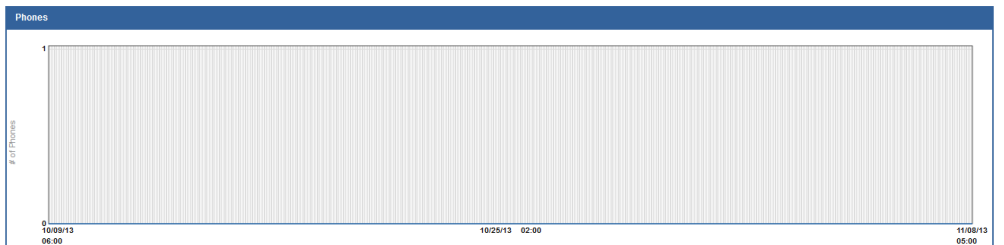
The number of *Phone Calls* in the *Phone Calls* graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the number of all the current wireless phone calls.

Phones

The *Phones* graph represents the aggregate number of all current registered phones. A phone is considered registered when it has been recognized by the network.

Figure 22 on page 55 illustrates the *Phones long term trend* graph.

Figure 22: Phones long term trend graph



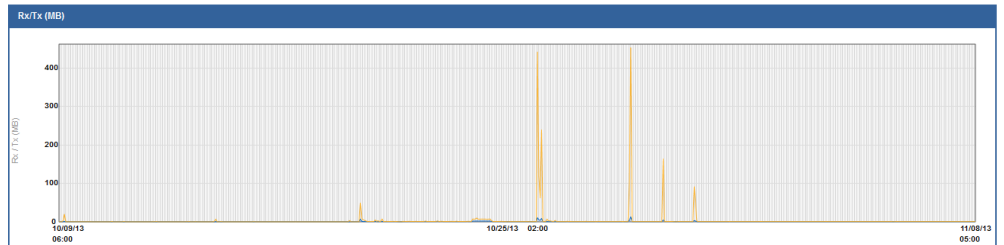
The number of registered *Phone* in the *Phone* graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the registered phones.

Rx/Tx

The *Receive data and Transmit data (Rx/Tx)* graph represents the data transferred in bytes.

Figure 23 on page 56 illustrates the *Receive data and Transmit data (Rx/Tx)* graph.

Figure 23: *Receive data and Transmit data (Rx/Tx) long term trend graph*



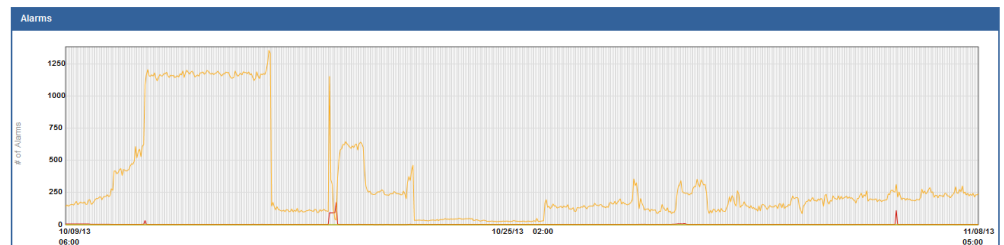
The number of Receive data and Transmit data (in bytes) can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the data transferred in bytes.

Alarms

The *Alarms* graph represents the aggregate number of all alarms on all polled controllers. The *critical* alarms are displayed in red color, *major* alarms in orange color and *minor* alarms in yellow color.

[Figure 24 on page 56](#) illustrates the *Alarms long term trend graph*.

Figure 24: *Alarms long term trend graph*



Hover the mouse pointer over a graph to view the number of the *Critical*, *Major*, and *Minor* alarms. Right click and select *Show Details* to view the details of the *Critical*, *Major* and *Minor* alarms.

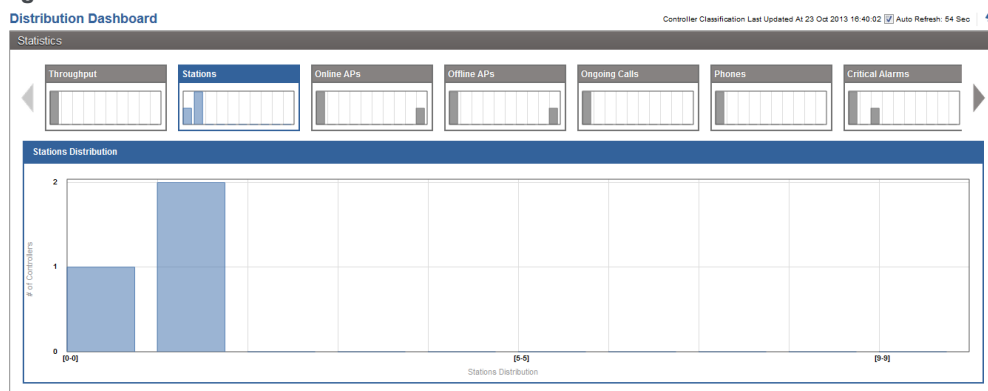
Distribution Dashboard

Monitor > Global Dashboard > Distribution Dashboard

The *Distribution Dashboard* displays data for the entire configured network on one chart; it displays the global graphs with available detailed breakdown of information. This graphing section of the distribution dashboard reflects the distribution of *throughput*, *stations*, *online and offline APs*, *phones and phone calls*, *alarms*, *noise*, *loss*, and *signals*. Each of these graphs is the collection of data for each topic, divided into ten bars per graph. To have these graphs automatically refresh every minute, *enable auto-refresh*.

Figure 25 on page 57 illustrates the *Distribution Dashboard* screen.

Figure 25: Distribution Dashboard



To interpret one of the 10 sections of a graph, move the mouse over a bar on the graph. The data range for the selected section with the number of controllers/stations that fall within in that data range is displayed. Perform a right-click on the graph and select *Show Details* to view the individual data for each graph.

In short, hover the mouse pointer over a graph to view further information. Right-click on the graphs, provides a drop-down list of available actions for that graph.

Throughput Distribution Graph

Click the small *Throughput* graph to see a larger version displayed in the middle of the screen. This graph represents the distribution of each controller's throughput over the range of the controller with the lowest throughput and the controller with the highest throughput. Throughput is graphed with integers and fractional values are rounded down. For example, if throughput is 10.5, it is counted in bar 9-10 (assuming bars are 9-10, 11-12 and so on). For example, the first bar could represent 1-10 Mbps, the second bar 11-20 Mbps, and the third 21-30Mbps. Two controllers could be operating 1-10 Mbps, three at 11-20, and two at 21-30Mbps. This is a simple way to scale network size.

Hover the mouse pointer over a bar to see the range included in that particular bar. To see throughput details for each controller, right-click on a throughput graph (either the large or small version) and select *Show Details*. Throughput details for each controller are displayed in Mbps.

Stations Distribution Graph

Click the small *Stations* graph to see a larger version displayed in the middle of the screen. This graph shows the distribution of wireless stations across the network managed by FortiWLM. The leftmost bars represent controllers supporting the fewest wireless stations and the right-most bars represent stations supporting the most wireless stations.

Online APs Distribution Graph

Click the small *Online APs* graph to see a larger version displayed in the middle of the screen. The graph represents the distribution of online APs on all controllers currently managed by FortiWLM that are up and running. This graph represents the number of APs on all controllers currently managed by FortiWLM that are up and running. The leftmost bars represent controllers supporting the fewest wireless stations and the right-most bars represent stations supporting the most wireless stations.

Offline APs Distribution Graph

Click the small *Offline APs* graph to see a larger version displayed in the middle of the screen. The graph represents the distribution for APs on all controllers managed by FortiWLM that are not running.

Ongoing Calls Distribution Graph

Click either small *Ongoing Calls* graph to see a larger version displayed in the middle of the screen. All ongoing calls are counted on every controller currently managed by FortiWLM, then that data is divided into 10 bars on this graph. Hover the pointer over a bar to see the data range included in that particular bar. To see details for each bar in the distribution, right-click an *ongoing call graph* (either the large or small version) and select *Show Details*. The details for each number of bars per controller are displayed.

Phones Distribution Graph

Click the small *Phones Distribution* graph to see a larger version displayed in the middle of the screen. Phones are connected to the wireless network that are either making calls at this time or not (same as associated phones). It represents the classification of controllers into ten groups based on number of wireless phones on the controller.

Critical Alarms Distribution Graph

Click a smaller *Alarms Distribution* graph to see a larger version displayed in the middle of the screen. The graph shows the distribution for all alarms on all controllers. Critical Alarms is marked as critical when the corresponding Notification Filter is created. This chart represents the classification of controllers into ten groups based on the number of critical alarms on the controller. Examples of critical alarms are *AP Down* and *Rogue AP Detected*.

High-Noise Radios Distribution Graph

This graph displays the distribution of radio noise. Click the small *High-Noise Radios* graph to see a larger version displayed in the middle of the screen. This graph shows the number of controllers whose noise value is greater than a set threshold (default is ≥ -70). Noise is defined as either random noise with no coherence or coherent noise introduced by the devices mechanism or processing. Noise level is calculated in each controller and represents the noise floor. No averaging method is used here and the noise level and noise floor are the same. The noise floor is represented in dBm which is a negative value.

High-Loss Radios Distribution Graph

This graph displays the distribution of radio loss. Click the small *High-Loss Radios* graph to see a larger version displayed in the middle of the screen. The graph shows the radio interface loss distribution for all radios on all controllers. Interface loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received. The graph represents the number of controllers whose loss value is greater than a set threshold (default is $\geq 50\%$). Interface Loss for a controller is the sum of Interface Loss of all APs. This graph represents the distribution of packet loss across all controllers over the last two minutes. Similarly to the Throughput graph, each bar represents a range of loss and how many controllers fall within that range. The network is performing best when most controllers are in the leftmost columns. There is a variable kept for each controller and so the transmit loss percentage for all unicast data frames is calculated for each controller using the formula $\text{Loss Percentage} = \frac{\text{Ack Fail Count}}{(\text{successful frames} + \text{Ack Fail Count})} * 100 (\%)$.

High-Loss Stations Distribution Graph

This graph displays the distribution of station loss. Click the smaller *High-Loss Stations* graph to see a larger version displayed in the middle of the screen. The graph represents the number of controllers with stations whose loss value is higher than a set threshold (default is $\geq 50\%$). Station loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received. This graph represents the distribution of packet loss across all stations over the last two minutes. Similar to the Throughput graph, each bar represents a range of loss and how many stations fall within that range. The network is performing best when most stations are in the leftmost columns. There is a variable kept for each station and so the transmit loss percentage for all unicast data frames is calculated for each station using the below formula:

Loss Percentage = Ack Fail Count / (successful frames + Ack Fail Count) * 100 (%).

Low-Signal Stations Distribution Graph

Click the smaller *Low-Signal Stations* graph to see a larger version displayed in the middle of the screen. The graph displays the signal distribution for stations on all controllers combined. This graph represents the number of controllers whose stations' RSSI value is less than a set threshold (default is <-80). Received Signal Strength Indication (RSSI) is a measurement of the power present in a received radio signal, aggregated across the entire network. The value reported is the measured signal strength in dBm averaged over 3 seconds.

Rogue APs Distribution Graph

This graph displays the distribution for rogue APs which are distributed on all network managed controllers. Click the smaller *Rogue APs* graph to see a larger version displayed in the middle of the screen. The rogue APs are calculated for the entire network (all controllers) and divided into 10 bars on this graph.

Another option is to display Rogue-AP related messages by clicking *Search* > providing the Keyword "rogue" > selecting *Alarms* > clicking *Search*.

Service Control

Monitor > Global Dashboard > Service Control

The *Service Control Summary* screen displays the list of services discovered in the network. By default, wireless services in all ESSIDs and all APs and wired services on VLAN 0 on the NM and controller's wired interface will be selected. To modify this, change the services that are discovered using "[Modifying Service Control Global Configuration](#)" on [page 157](#).

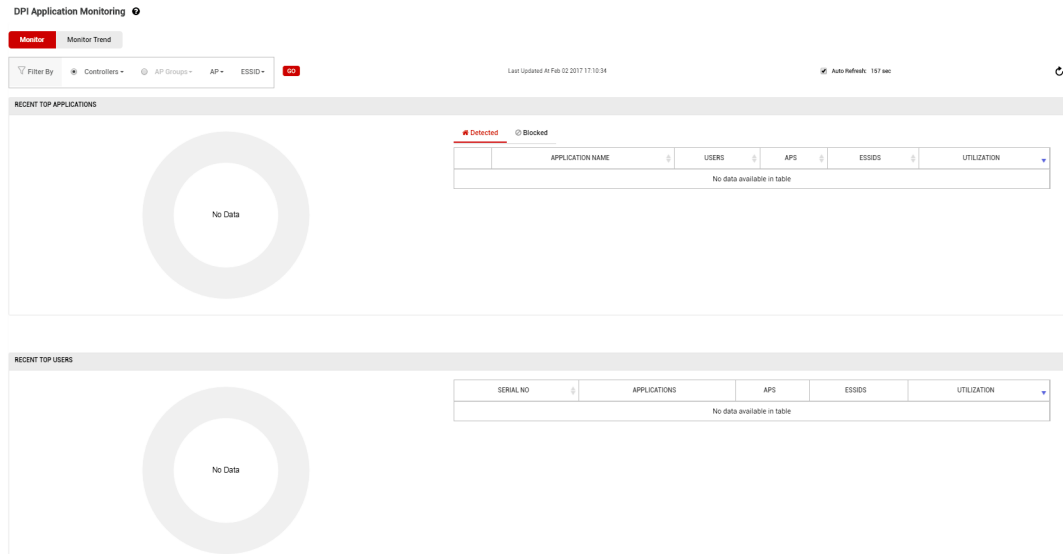
The *Service Control Summary* consists of the following sections:

1. **Statistics:** The Statistics section provides a graphical representation (pie chart) of the services discovered in the network. The area of each sector is proportional to the percentage of the number of services by each category against the total number of services. The following two types of services are graphically represented:
 - **Services Chart:** The services chart provides the service types that are discovered in the network. The chart is color coded based on the service types.
 - **Wired/Wireless Chart:** This chart is about the services discovered in the network based on the Wired or Wireless network. The chart is color coded based on the network type, Wired or Wireless.
2. **Service Details:** The Service Details section provides the information of the services that are discovered in the network. The *Controller*, *Service*, *Service Name*, *Service Type*, *Location*, *Node Name*, *Source Type*, and *Source* details are displayed in this section.

Application Visibility

You can monitor the traffic of top 10 applications used in your network. The Monitor > Global Dashboard > Application Visibility dashboard provides detailed graph of top 10 applications.

Figure 26: Application Visibility Dashboard



The dashboard shows graphical display of traffic usage by Applications or Users (Clients).

- The *Pie chart* displays top 10 applications. Hover over pie slices to see traffic usage (in percentage) of an application.
- *Tabular data* with the list of top 10 applications. For each application, you can view the following:
 - Number clients using the application
 - Number of APs serving the clients using the application
 - Number of ESSID connected to clients using the application
 - Total traffic utilization in MB.
- The *Trends* graph displays traffic usage in different intervals (2 hour, 1 day, 1 week, 1 month, and custom interval for a specified date range).



The trend graph data is maintained only for the last 30 days.

Device Dashboard

The *Device Dashboard* provides at-a-glance system information to the following dashboards available towards the left panel of each page:

- “*Controller Dashboard*” on page 62
- “*AP Dashboard*” on page 63
- “*Nplus1 Clusters*” on page 64

Controller Dashboard

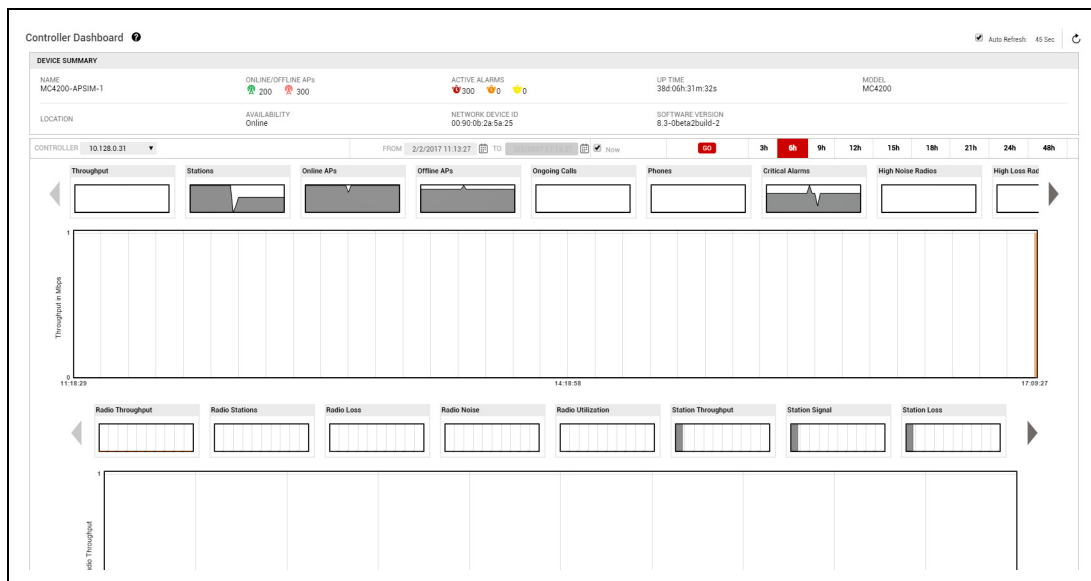
Monitor > Device Dashboard > Controller Dashboard

The *Controller Dashboard* screen displays an in-depth information about the controller's activity. It provides the graphical representation of the *Throughput Trend*, *Stations*, *Online APs*, *Offline APs*, *Ongoing Calls*, *Registered Phones*, *Critical Alarms*, *High-Noise Radios*, *High-Loss Radios*, *High-Loss Stations*, *Low-Signal Stations*, and *Rogue APs* of the selected controllers that are managed by *FortiWLM*. The results for the controller are displayed in the upper graphs and results per radio is displayed in the lower set of graphs.

Figure 27 on page 63 illustrates the *Controller Dashboard* screen.

1. Navigate to *Monitor > Device Dashboard > Controller*.
2. In the *Controller Dashboard* screen, select a controller IP address from the *Controller Selection* drop-down list. The details such as *name*, *location*, *availability status*, *the number of online or offline APs connected*, *the alarms raised*, and *other details* for the selected controller is displayed.

Figure 27: Controller Dashboard



3. The *Controller Dashboard* screen provides the graphical representation of the *Throughput Trend*, *Stations*, *Online APs*, *Offline APs*, *Ongoing Calls*, *Registered Phones*, *Critical Alarms*, *High-Noise Radios*, *High-Loss Radios*, *High-Loss Stations*, *Low-Signal Stations*, and *Rogue APs* of the selected controllers that are managed by *FortiWLM*.
4. The upper graphs display the results for the controller or trend graphs for the selected controller. *Click* a smaller upper graph to see a larger version displayed in the middle of the screen.
5. The lower graphs are distribution state graphs for a respective parameter at a given time. *Click* a smaller lower graph to see a larger version displayed in the middle of the screen.
6. The trends based on controller selection is monitored by selecting the trend duration. The time period can be modified from 1 to 48 hours by selecting the Trend Interval or by selecting the “*From*” and “*To*” duration of time.

See the **Controller Dashboard** screen (*Monitor > Device Dashboard > Controller*) in Online Help for detailed information on the *Controller Trends* and *Distribution Trends*.

AP Dashboard

Monitor > Device Dashboard > Controller Dashboard

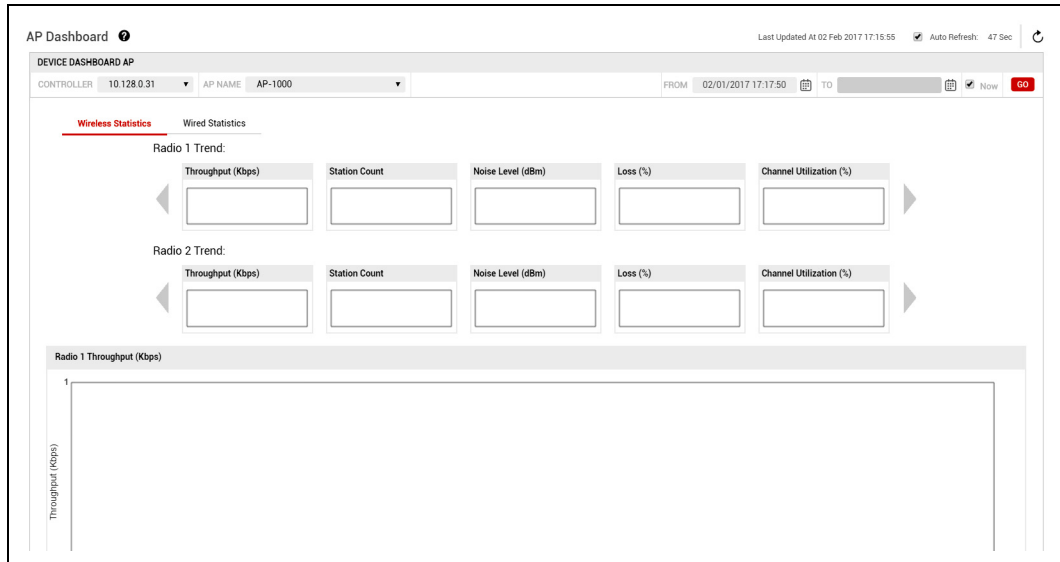
The *AP Dashboard* screen displays an in-depth information about the AP activity. It provides the graphical representation of the *Throughput*, *Stations*, *Noise Level*, *Loss%*, and *Channel*

Utilization% for each of the radio on AP connected to the controller which is managed by *For-tiWLM*. The results for the radio on AP is graphically displayed on the top portion of the window and *Trends Per radio* in the lower portion of the window.

Figure 28 on page 64 illustrates the *AP Dashboard* screen.

1. Click *Monitor > Device Dashboard > AP*.

Figure 28: AP Dashboard



2. In the *AP Dashboard* screen, select a controller IP address from the *Controller* drop-down list. The controller selection provides the list of APs located on the selected controller.
3. Select an *AP* from the *AP Name* drop-down list.
4. Select the time period by selecting the “*From*” and “*To*” duration of time. The time interval cannot be more than 1 day. Select the *Refresh* icon.
5. The results for the radio on AP is displayed in the graphs on the top portion of the window and *Trends Per radio* in the lower portion of the window.
6. The number of *Radios* displayed varies from one AP to Other. To illustrate, If the AP is Teton, a third set of graphs are displayed.

See the **AP Dashboard** screen (*Monitor > Device Dashboard > AP*) in Online Help for detailed information on *the AP Trends*.

Nplus1 Clusters

Monitor > Device Dashboard > Nplus1 Clusters

The Nplus1 clusters allow a standby Nplus1 slave controller in the same subnet to monitor and failover more than one master controller.

A set of master controllers and a standby slave controller are configured via static IP addressing to reside in the same subnet, and are considered to be an N+1 cluster. The standby slave monitors the availability of the master controllers in the cluster by receiving advertisement messages sent by the masters over a well known UDP port at expected intervals. If five successive advertisements are not received, the standby slave changes state to an active slave, assumes the IP address of the failed master, and takes over operations for the failed master. Because the standby slave already has a copy of the master's latest saved configuration, all configured services continue with a short pause while the slave switches from standby to active state.

While in the active slave role, the slave controller's cluster monitoring activities are put on hold until the failed master rejoins the cluster. An active slave detects the restart of a master through ARP (Address Resolution Protocol). When the active slave is aware of the master's return (via the advertisement message) it relinquishes the master's IP address and then returns to the standby state. The now-passive slave will not fail over for the same master until a WTR (Wait to Restore) is completed.

If it is necessary for the failed master to be off-line for a lengthy interval, the administrator can manually set the active slave back to the standby slave, thereby ensuring the standby slave is able to failover for another master.

In most cases with a cluster of N+1 Masters, the APs all have to be in L3 Connectivity mode, but if you only have one Master and one Slave unit (N=1) the APs can be in L2 connectivity mode. In this case, while the Master unit is active the Slave unit will not take AP registration so the AP will always go to the correct controller.

FortiWLM monitors the overall health of the cluster by looking at the *Master to Slave* transitions. You can add slave controllers in the *FortiWLM* and view the masters for the *Nplus1 cluster* to monitor the events related to master or slave transition.

The controller is configured to *Master* or *Slave* through the *System Director* CLI. *FortiWLM* allows you to add the configured slave and master controllers to the nms-server. This is achieved by navigating to, *Inventory > Devices > Controllers > Add* icon.

To view the Nplus1 state of the selected controller, navigate to *Devices > Controllers > Select a controller > Click on View Details > Nplus1 State* option.

You can upgrade the *Nplus1 clusters* by selecting the *Upgrade Group* as *Nplus1 Clusters* in the *Current Upgrades* screen (*Inventory > Software Upgrades > Current Upgrades > Add icon > Upgrade Group*).



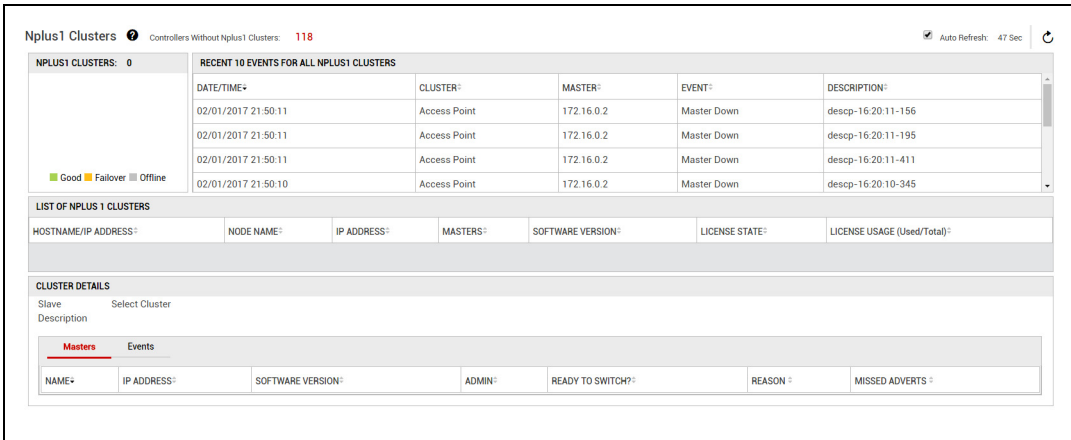
Slave controllers cannot be registered to a service profile. The status is displayed as *Sync Failed* when registered to a slave controller.

The *Nplus1 Clusters* screen in the *Monitor* menu allows you to view the history of transitions for the *Nplus1 cluster*.

Figure 29 on page 66 illustrates the *Nplus1 Clusters* screen.

1. Navigate to *Monitor > Device Dashboard > Nplus1*.

Figure 29: *Nplus1 Clusters*



2. The *Nplus1 Clusters* screen is divided into the following four sections:

- *Nplus1 Clusters* section
- Recent 10 events for all *Nplus1 Clusters*
- List of *Nplus1 Clusters*
- Cluster Details

Nplus1 Clusters section

This section provides the graphical representation of the *Good*, *Failover* and *Offline* clusters in pie-chart. Further details of each cluster are displayed by hovering the mouse pointer over each block.

- **Good Clusters:** These are *Passive Slave Controllers* where, the *slave controller* is ready to take control over the *master controller*. The *Good Clusters* are represented in *Green* color in the pie chart.
- **Failover Clusters:** These are *Active Slave Controllers* where, the *slave controller* takes control over the failed *master controller*. The *Failover Clusters* are represented in *Yellow* color in the pie chart.
- **Offline Clusters:** These are *Slave Controllers* which are neither *Active* nor *Passive*. When the master controller goes down, there is no *slave controller* to take control over the *master controller*. The *Offline Clusters* are represented in *Red* color in the pie chart.

Recent 10 events for all Nplus1 Clusters

This section displays the recent Nplus1 related events for all the clusters in the nms-server. It provides the details of the Master controller. The primary details are as follows:

Field	Description
Date/Time	Displays the date/time at which the event occurred.
Cluster	Displays the cluster to which the notification belongs to.
Master	Displays the IP address of the master controller.
Event	Displays the event of the master controller, if the master controller is down or up.
Description	Displays the event description.

List of Nplus1 Clusters

This section provides the list of clusters added in the *FortiWLM* server. It displays the *Good*, *Failover* and *Offline* clusters. Select any one of the *Nplus1 cluster* type (*Good*, *Failover* or *Offline Clusters*) from the *Nplus1 Clusters* section (graph), the list of Nplus1 Clusters heading is modified to the selected type of cluster as per the selection.

Field	Description
Host Name/IP Address	Displays the host name of the slave controller. Select a host name link, the details are displayed in the <i>Cluster Details</i> section. See " Cluster Details " on page 68.
Node Name	Displays the name of the slave controller.
IP Address	Displays the IP address of the slave controller.
Masters	Displays the number of master controllers in the cluster.
Software Version	Displays the software version of the slave controller.

Field	Description
Wait To Restore	Displays the <i>Wait to Restore</i> countdown timer that is used to count down before the <i>Standby slave</i> can again take over the role of a <i>Master</i> unit it recently relinquished.
Master Timeout	Displays the timeout of the master controller.
License State	Displays the licensed state of the <i>Slave Controller</i> . The types are as follows: <ul style="list-style-type: none"> • Licensed • Unlicensed
License Usage (Used/ Total)	Displays the total number of the Nplus1 licenses and the number of licenses used on the slave controller.

Cluster Details

The *Cluster Details* section displays the Host Name of the selected slave controller from the *List of Nplus1* table along with the description that can be modified by the *Edit* selection. The *Masters* and *Events* of the slave are viewed by selecting any slave controller from the *List of Nplus1 Clusters* table.

Masters Tab

Select any slave controller from the *List of Nplus1* table to view the Masters of the selected slave. The following fields are displayed:

Field	Description
Name	Displays the host name of the master controller.
IP Address	Displays the static IP address assigned to the master controller.
Software Version	Displays the software version of the master controller.
Admin	Displays the status of Nplus1 clusters on the master: <ul style="list-style-type: none"> • <i>Enable</i>—Nplus1 clusters have been enabled on the Master Controller. • <i>Disable</i>—Nplus1 clusters have been disabled on the Master Controller.
Switch	The ability of the slave to assume the active slave for the master: <ul style="list-style-type: none"> • <i>Yes</i>—Slave and master model/<i>FortiWLM</i> version number is compatible. • <i>No</i>—Slave and master model/<i>FortiWLM</i> version number are incompatible or the administrator has disabled Nplus1 on the master.

Field	Description
Reason	<p>If <i>Switch</i> is <i>No</i>, describes why switch cannot be made:</p> <ul style="list-style-type: none"> • <i>Down</i>: The master has been disabled by the user. • <i>No Access</i>: The passive slave was not able to access the master because it did not receive a copy of the configuration. This is a rare message that occurs if show nplus1 is executed almost immediately after adding a controller.
Missed Adverts	Displays the number of consecutively missed (not received) advertisements (a maximum of 5 triggers a failover if the Switch field is Yes).

Events Tab

Select any slave from the *List of Nplus1* table to view the *Events* of the selected slave. The following fields are displayed:

Field	Description
Date/Time	The date and time at which the event occurred.
Master	Displays the device name.
Description	Displays the Event description.

Status Bar

The *Status Bar* displays the Icons for the following Nplus1 Clusters with a tool tip label:

- Good Clusters
- Failover Clusters
- Offline Clusters

Select one of the above mentioned *Nplus1 Clusters* icon, a summary of the selected *Nplus1 Cluster* is displayed in a separate window as a pop-up screen. The *Nplus1 Clusters* screen and the status bar use the same aggregated data. All the links or pop-up from this page and status bar display the current data.

Fault Dashboard

Monitor > Fault Dashboard > Fault Management

The *Alarms and Events* interface is now available via a single dashboard as the *Fault Management*. The dashboard includes alarms and events for access points, controllers and NM. Fault management allows you to detect and notify faults encountered in the network.

[Figure 30 on page 70](#) illustrates the *Fault Management* screen.

To access *Fault management*, perform the following steps:

1. Select Monitor > Fault Dashboard > Fault Management.

Figure 30: Fault Management

The screenshot shows the 'Fault Management' interface. At the top, there are tabs for 'Alarms', 'Events', and 'Storage Info'. Below these, there are sub-tabs for 'Active Alarms', 'History Alarms', and 'Definition'. The 'Active Alarms' tab is selected. The interface includes a search bar, a date range selector (FROM 02/01/2017 17:19:11 TO 02/02/2017 17:19:11), and a time range selector (2h, 4h, 1d, 1w, 1m). There are also buttons for 'CSV', 'RESYNC', 'CLEAR', 'ACKNOWLEDGE', and 'Filter Active Alarms'. The main table displays a list of active alarms with columns for 'ALARM NAME', 'SEVERITY', 'SOURCE', 'FDN', 'CONTROLLER NAME', 'RAISED AT (IST)', 'DESCRIPTION', 'ACKNOWLEDGED', and 'ACTIONS'. The table contains 8 rows of data, all showing 'AP Down' alarms with 'Critical' severity.

ALARM NAME	SEVERITY	SOURCE	FDN	CONTROLLER NAME	RAISED AT (IST)	DESCRIPTION	ACKNOWLEDGED	ACTIONS
AP Down	Critical	Access Point	SD-AP-877	10.128.0.40	02/02/2017 16:30:42	AP [<AP-877> MAC address<00:0c:e6:52:02:75> IP<10.128.134.22>] is down	No	
AP Down	Critical	Access Point	SD-AP-887	10.128.0.40	02/02/2017 16:30:42	AP [<AP-887> MAC address<00:0c:e6:52:02:85> IP<10.128.134.32>] is down	No	
AP Down	Critical	Access Point	SD-AP-882	10.128.0.40	02/02/2017 16:30:42	AP [<AP-882> MAC address<00:0c:e6:52:02:80> IP<10.128.134.27>] is down	No	
AP Down	Critical	Access Point	SD-AP-892	10.128.0.40	02/02/2017 16:30:41	AP [<AP-892> MAC address<00:0c:e6:52:02:90> IP<10.128.134.37>] is down	No	
AP Down	Critical	Access Point	SD-AP-897	10.128.0.40	02/02/2017 16:30:41	AP [<AP-897> MAC address<00:0c:e6:52:02:95> IP<10.128.134.42>] is down	No	
AP Down	Critical	Access Point	SD-AP-876	10.128.0.40	02/02/2017 16:30:38	AP [<AP-876> MAC address<00:0c:e6:52:02:74> IP<10.128.134.21>] is down	No	
AP Down	Critical	Access Point	SD-AP-881	10.128.0.40	02/02/2017 16:30:37	AP [<AP-881> MAC address<00:0c:e6:52:02:79> IP<10.128.134.26>] is down	No	

2. The *Fault Management* screen is divided into the following tabs:

- “[Alarms](#)” on [page 70](#)
- “[Events](#)” on [page 76](#)
- “[Storage Info](#)” on [page 79](#)

Alarms

An *Alarm* is a notification of faults that occur over the course of time for an object. An alarm is either in *Active State* or *Cleared State*. When alarms are generated, you can either *Acknowledge* or *Clear the alarm* by simply checking the box alongside the desired alarm and clicking the appropriate button towards the bottom of the window. For an object, a new alarm cannot be raised until the old alarm is cleared. However, the same alarm on same object can be raised with different severity. During such scenarios, the new alarm will clear the old alarm.

- *Clear*—Moves the alarm from the *Active Alarms* table into the *Alarm History* table.
- *Acknowledge*—Marks the alarm as acknowledged in the *Acknowledged* column.

As seen in the figure above, the *Active Alarms* table provides several columns as described below:

Column	Description
Alarm Name	The name of the alarm triggered.
Severity	<p>Displays the <i>Severity</i> of the alarm. The severity types are as follows:</p> <ul style="list-style-type: none"> • Critical Alarms <ul style="list-style-type: none"> • Critical Alarms are represented by <i>red</i> color and indicates the need for immediate action. • Typical critical alarms are generated either when a controller or AP is down, or when a rogue AP is detected. The <i>Rogue</i> alarm is raised when the <i>Wired Rogue</i> is detected. • Major Alarms <ul style="list-style-type: none"> • Major Alarms are represented by <i>orange</i> color and indicates the need for action when ever required. • Typical major alarms are displayed due to <i>Authentication failure</i>. • Minor Alarms <ul style="list-style-type: none"> • Minor Alarms are represented by <i>yellow</i> color and does not require any action. • Typical minor alarms are displayed due to MIC errors. • Information Alarms <ul style="list-style-type: none"> • Information Alarms are represented by <i>blue</i> color and is for information only. It does not require any action.
Source	<p>Displays the Source name through which the alarm is raised. The following are the source names:</p> <ul style="list-style-type: none"> • Controller • Access Point • NM

Column	Description
FDN (Full Distinguished Name)	<p>The name of the device that triggered the alarm.</p> <p>Full Distinguished Name (FDN) identifies the name of the device that triggered the alarm.</p> <p>The abbreviations of <i>Fortinet Products</i> (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address.</p> <p>Note:</p> <p>The FDN received by SD applications are not supported by FortiWLM.</p>
Controller	Displays the controller IP address.
Raised At	<p>The date and time at which the alarm was triggered.</p> <p>Note:</p> <p>The time displayed will be in IST time zone. This can be modified by selecting the <i>Change Timezone</i> option.</p>
Description	Detailed information regarding the alarm, including identifying device details.
Acknowledged	Indicates whether the alarm has been flagged as Acknowledged.
Actions	All the AP related alarms display the <i>AP Location</i> icon in the <i>Actions</i> column. Select the <i>Show AP Location</i> icon. The <i>AP Locator</i> screen is displayed. The <i>AP Locator</i> screen displays the selected AP located on the floor.

Modifying Alarm Definitions

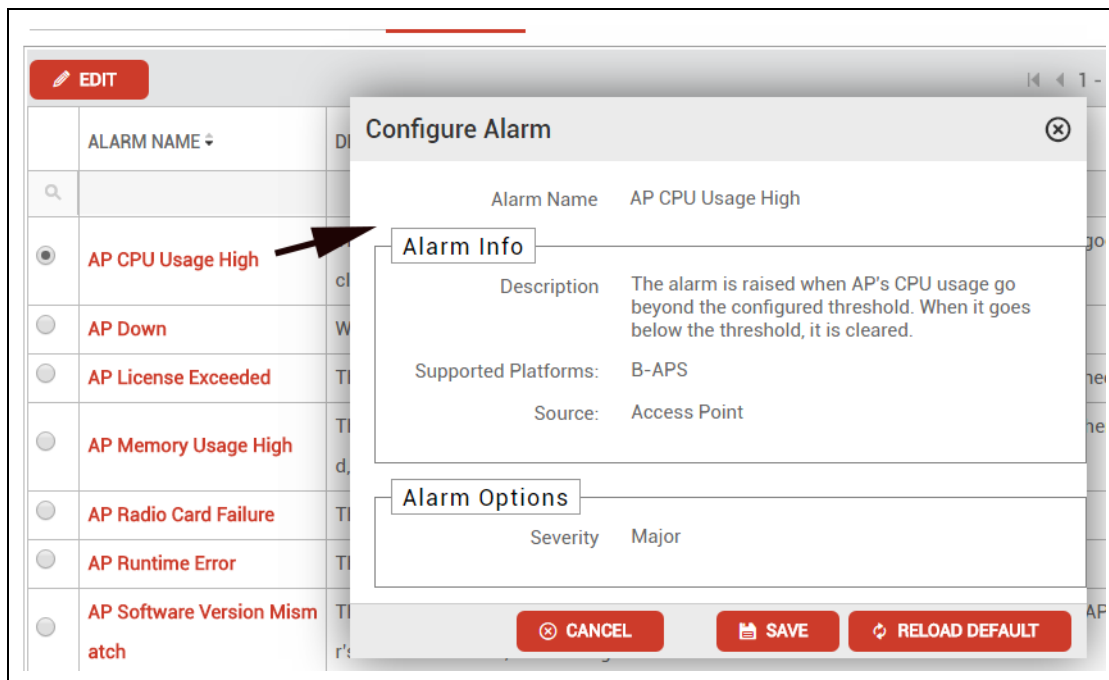
While *FortiWLM* provides a list of pre-configured alarms, you can also customize some of the attributes/triggering conditions for each of the alarm type. This can be performed via the *Alarms > Definition* tab. [Figure 31 on page 73](#) illustrates the *Alarm Definitions*.

Figure 31: Alarm Definitions

Fault Management ?						
<div>Alarms Events Storage Info</div>						
<div>Active Alarms History Alarms Definition</div>						
<div> <div>EDIT</div> <div>1 - 41 of 41</div> </div>						
ALARM NAME	DESCRIPTION	SEVERITY	SOURCE	TRIGGERING CONDITION	TRIGGERING THRESHOLD	
<input checked="" type="radio"/> AP CPU Usage High	The alarm is raised when AP's CPU usage go beyond the configured threshold. When it goes below the threshold, it is cleared.	Major	Access Point	N/A	N/A	
<input type="radio"/> AP Down	When an AP goes offline, the alarm is raised, and cleared when the AP comes online	Critical	Access Point	N/A	0	
<input type="radio"/> AP License Exceeded	This alarm is raised when an AP is connected to controller after the license limit is reached.	Critical	Access Point	N/A	0	
<input type="radio"/> AP Memory Usage High	The alarm is raised when AP's Memory usage goes beyond the configured threshold. When it goes below the threshold, it is cleared.	Major	Access Point	N/A	N/A	
<input type="radio"/> AP Radio Card Failure	The alarm is raised when a radio card is down. It is cleared when the card is fixed	Critical	Access Point	N/A	0	
<input type="radio"/> AP Runtime Error	The alarm is raised when AP300 reboots due to internal error	Minor	Access Point	N/A	0	
<input type="radio"/> AP Software Version Mismatch	The firmware version on the AP does not match the version on the controller. When the AP gets upgraded to Controller's firmware version, the alarm gets cleared	Critical	Access Point	N/A	0	
<input type="radio"/> AP Wireless Interface Down	An alarm is raised when the Radio fails to turn operational during Initial boot up. This occurs due to some Hardware issue on the AP Radio. When the radio gets recovered, the alarm gets cleared	Critical	Access Point	N/A	0	

As shown above, each alarm comprises of a default predetermined *severity level*, *source*, *trigger condition*, *triggering threshold*, *SNMP*, and *syslog* but these values can be modified by selecting the desired *Alarm Name* followed by selecting the *Edit* option. The respective alarm details are displayed in the *Configure Alarm* window, as seen in [Figure 32 on page 74](#).

Figure 32: *Configure Alarm*



Modify the *Threshold Trigger Condition* and click *Save* when finished. If desired, you can click *Reload Default* to reset the alarms configuration to its original values.



The *Threshold* field's units will vary depending on the alarm selected—for example, when modifying *AP Memory Usage High*, the *Threshold* is measured in percentage of overall system memory (and defaults to 70%). However, in an alarm such as *Link Down*, no threshold is needed at all, as it is a binary alarm (i.e., it is triggered when a link to an AP goes down—there is no percentage involved).

Filter History Alarms

The *Filter History Alarms* allows you to filter alarms based on various parameters. Any of the following parameters can be selected from the *Filter History Alarms* popup. The table can be filtered using more than one parameter. For Example: You can filter alarms by providing the Alarm Name, FDN, and Source.

Column	Description
Alarm Name	Provide the alarm name.

Column	Description
Severity	<p>Select the <i>Severity</i> of the alarm. The severity types are as follows:</p> <ul style="list-style-type: none"> • Critical Alarms <ul style="list-style-type: none"> • Critical Alarms are represented by <i>red</i> color and indicates the need for immediate action. • Typical critical alarms are generated either when a controller or AP is down, or when a rogue AP is detected. The <i>Rogue</i> alarm is raised when the <i>Wired Rogue</i> is detected. • Major Alarms <ul style="list-style-type: none"> • Major Alarms are represented by <i>orange</i> color and indicates the need for action when ever required. • Typical major alarms are displayed due to <i>Authentication failure</i>. • Minor Alarms <ul style="list-style-type: none"> • Minor Alarms are represented by <i>yellow</i> color and does not require any action. • Typical minor alarms are displayed due to MIC errors. • Information Alarms <ul style="list-style-type: none"> • Information Alarms are represented by <i>blue</i> color and is for information only. It does not require any action.
Source	<p>Select the <i>Source</i> name through which the alarm is raised. The following are the source names:</p> <ul style="list-style-type: none"> • Controller • Access Point • NM

Column	Description
FDN (Full Distinguished Name)	<p>Provide the name of the device that triggered the alarm.</p> <p>Full Distinguished Name (FDN) identifies the name of the device that triggered the alarm.</p> <p>The abbreviations of <i>Fortinet Products</i> (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address.</p> <p>Note:</p> <p>The FDN received by SD applications are not supported by FortiWLM.</p>
Controller	Provide the controller IP address.
Description	Provide a detailed information about the alarm raised followed by alarm cleared.
Acknowledged	Provide if the user has acknowledged the alarm raised. The options are Yes or No. The default is No.

1. Select *Save* option to filter the history alarms with the parameters mentioned in the above table.
2. Select *Reset* option to reset all the fields mentioned in the above table.
3. Select *Cancel* to close the filter history alarms popup.

See the **Fault Management** screen (*Monitor > Fault Dashboard > Fault Management*) in Online Help for detailed information on *configuring Alarms* and *Alarm definitions*.

Events

The *Events* are significant occurrences that take place on the E(z)RF-managed network. They are similar to alarms. The Event instances are generated based on a condition and can be generated multiple times. However, while alarms typically require some form of user intervention to resolve the problem, events simply provide an indication that a change has been made. [Figure 33 on page 77](#). illustrates the *Fault Management - Events* screen.

Figure 33: Fault Management - Events

EVENT NAME :	SEVERITY :	SOURCE :	FDN :	CONTROLLER NAME :	GENERATED AT(IST) :	DESCRIPTION :
Controller Backup failed	Major	NM	NM-10.128.0.31	10.128.0.31	02/02/2017 17:05:58	Configuration backup failed for controller 10.128.0.31, Connection timed out
Controller Backup failed	Major	NM	NM-10.33.63.21	10.33.63.21	02/02/2017 17:05:58	Configuration backup failed for controller 10.33.63.21, Connection timed out
Alarm History Reached Threshold	Major	Access Point	fdn-11.35.03-431	172.16.0.2	02/02/2017 17:05:03	descp-11.35.03-431
Interference detected	Major	Access Point	fdn-11.35.03-120	172.16.0.2	02/02/2017 17:05:03	descp-11.35.03-120
Certificate Error	Information	Access Point	fdn-11.35.03-44	172.16.0.2	02/02/2017 17:05:03	descp-11.35.03-44
Certificate Error	Information	Access Point	fdn-11.35.03-369	172.16.0.2	02/02/2017 17:05:03	descp-11.35.03-369
CAC limit reached	Major	Access Point	fdn-11.35.03-226	172.16.0.2	02/02/2017 17:05:03	descp-11.35.03-226
DFS Channel Update	Major	Access Point	fdn-11.35.02-264	172.16.0.2	02/02/2017 17:05:03	descp-11.35.02-264
MIC Counter Measure Activation	Major	Access Point	fdn-11.35.03-313	172.16.0.2	02/02/2017 17:05:03	descp-11.35.03-313

The table below provides a brief description of the columns provided in the *Events* table.

Column	Description
Event Name	The name of the event triggered.
Severity	The severity level; can range from <i>Information</i> , <i>Minor</i> , <i>Major</i> , <i>Critical</i> .
Source	Displays the source name through which the event is raised. The following are the source names: <ul style="list-style-type: none"> Controller Access Point NM
FDN	The name of the device that triggered the event. <i>Full Distinguished Name</i> (FDN) identifies the name of the device that triggered the event. The abbreviations of <i>Fortinet Products</i> (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address. Note: The FDN received by SD applications are not supported by FortiWLM.

Column	Description
Raised At	The date and time at which the event was triggered. Note: The time displayed will be in IST time zone. This can be modified by selecting the <i>Change Timezone</i> option.
Detail	Detailed information regarding the event, including identifying device details.

Modifying Event Definitions

While *FortiWLM* provides a list of pre-configured events, you can also customize some of the attributes/triggering conditions for each of the event type. This can be performed via the *Events > Definition* tab. Each event has a predetermined severity level, trigger condition, and threshold, but these values can be modified by selecting the desired *Event Name* followed by selecting the *Edit* option. The respective event details are displayed in the *Configure Event* window.

Modify the *Threshold Trigger Condition* and click *Save* when finished. If desired, you can click *Reload Default* to reset the event's configuration to its original values.

Filter Events

The *Filter Events* allows you to filter events based on various parameters. Any of the following parameters can be selected from the *Filter Events* popup. The table can be filtered using more than one parameter. For Example: You can filter alarms by providing the Event Name, FDN, and Source.

Column	Description
Event Name	Provide an event name.
Severity	Select the severity level; can range from <i>Information</i> , <i>Minor</i> , <i>Major</i> , <i>Critical</i> .
Source	Select the source name through which the event is raised. The following are the source names: <ul style="list-style-type: none"> • Controller • Access Point • NM

Column	Description
FDN	<p>Provide the name of the device that triggered the event.</p> <p><i>Full Distinguished Name</i> (FDN) identifies the name of the device that triggered the event.</p> <p>The abbreviations of <i>Fortinet Products</i> (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address.</p> <p>Note:</p> <p>The FDN received by SD applications are not supported by FortiWLM.</p>
Controller	Provide the <i>Controller IP Address</i> .
Detail	Provide the complete or partial description about the event generated.

1. Select *Save* option to filter the events with the parameters mentioned in the above table.
2. Select *Reset* option to reset all the fields mentioned in the above table.
3. Select *Cancel* to close the filter events popup.

See the **Fault Management** screen (*Monitor > Fault Dashboard > Fault Management*) in Online Help for detailed information on *configuring Events* and *Event definitions*.

Storage Info

The Storage Info displays the *Storage Configuration* details of the *Alarms* and *Events*.

- [“Events - Storage Configuration” on page 79](#)
- [“History Alarms - Storage Configuration” on page 80](#)

Events - Storage Configuration

The *Events - Storage* configuration displays the following details:

Field	Description
Storage Capacity	Displays the maximum number of Events that can be stored in the database. The maximum storage capacity is 4000000 rows.
Current Usage	Displays the current usage of <i>Events</i> storage in percentage

Field	Description
<p>Purge Options</p> <p>Purge is a scheduled operation that allows you to delete records following a configurable predefined setting. The maximum number of records to store and the number of records to retain is configured in the database. Purge operation is enforced, once the database crosses the configured number of records. The most former record is deleted from the database.</p>	
Number of events to keep after every purge	Displays the percentage of <i>Events</i> to be retained after purge.
Schedule Purge	Displays the scheduled time of purge for the <i>Events</i> . Select the desired time from the drop-down list.
Enable Auto System Purge	System will purge events once usage reaches 99%.

History Alarms - Storage Configuration

The *History Alarms - Storage* configuration displays the following details:

Field	Description
Storage Capacity	Displays the maximum number of Alarms that can be stored in the database. The maximum storage capacity is 2000000 rows.
Current Usage	Display current usage of historical alarm storage in percentage.
<p>Purge Options</p>	
Number of History Alarms to keep after every purge	Display percentage of historical alarm to retain after purge.
Schedule Purge	Displays the scheduled time of purge for the <i>History Alarms</i> . Select the desired time from the drop-down list.
Enable Auto System Purge	System will purge historical alarms once usage reaches 99%.

Station Activity

The *Station Activity* of the *Monitor* menu displays the performance trends for a specific station. An intuitive graphical display of the *throughput, signal strength, loss, and airtime utilization trends* are plotted for the selected station. The station history can be viewed and exported in CSV format (comma separated values) by selecting the CSV option. The event types are filtered either based on the station event type or by selecting the controller, event severity, event Id, and MAC address. The *Station Activity* comprises of the below mentioned dashboards:

- “*Station Trend Dashboard*” on page 81
- “*Station Activity Log*” on page 84

Station Trend Dashboard

Monitor > Station Activity > Station Trend Dashboard

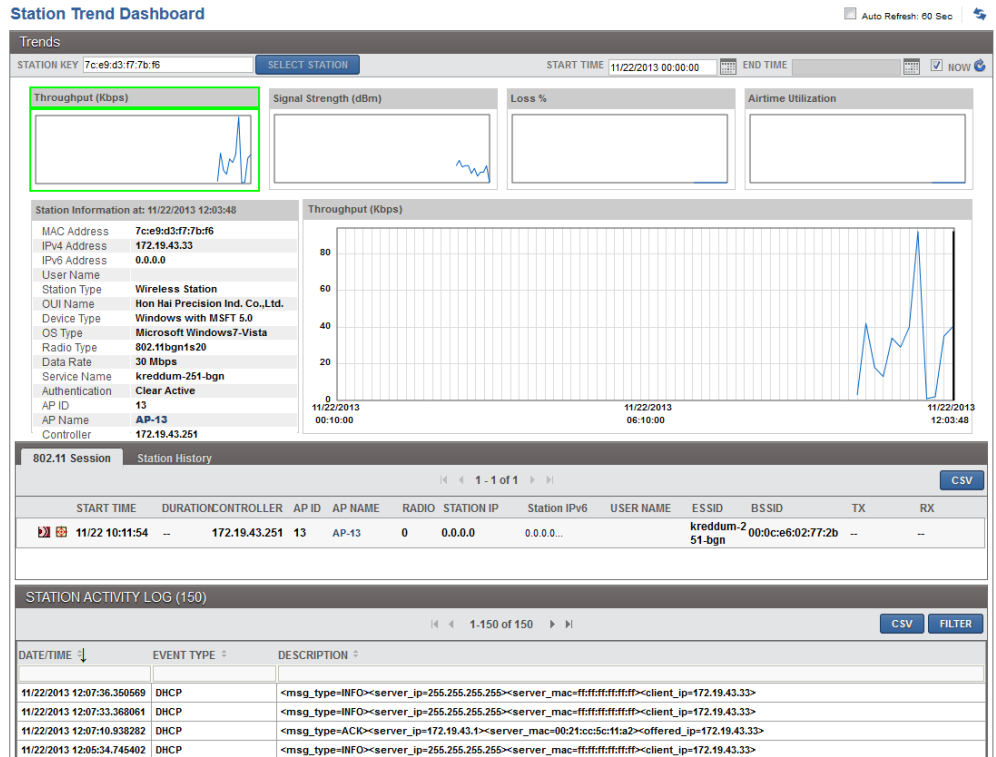
The *Station Trend Dashboard* displays a variety of performance trends for a specific station or all stations for a specific controller. The graphs on the station trend dashboard require a MAC address or the user name. If you don't know the MAC address, use the *Search* function (*Monitor > Tools > Search*) to find a station by entering keywords related to that station. Copy the MAC address and use it as input for this *Station Trend Dashboard*.

Figure 34 on page 82 illustrates the *Station Trend Dashboard* screen.

To see information for an individual station, follow these steps:

1. Click *Monitor > Device Dashboard > Station*.

Figure 34: Station Trend Dashboard



2. In the *Station Trend Dashboard* screen, obtain a *Station Key* by selecting the *Select Station* option. The IP address of the selected *Station* is displayed as the *Station Key*.
3. Provide a *Start Time* and *End Time* in the format 01/08/2009 09:14:51 (the date followed by time in the format hh:mm:ss). Optionally, use a calendar to select the date and time. To use the current time, check *Now*. Note that the start and end times cannot be more than 24 hours apart. followed by selecting the *Refresh* option.
4. The following sections are displayed.

Charts

Station Throughput Chart

The *Station Throughput* chart displays stations combined transmitted and received bytes during a 10 minute interval. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. Right-click and select *Show Details* to view the Throughput details.

Signal Strength Chart

The *Signal Strength* chart displays the signal strength (dBm) for this station in the time period indicated. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. The chart is updated approximately every 10 minutes. Right-click and select *Show Details* to view the Signal Strength details.

Loss% Chart

The *Loss%* chart displays the station's transmit loss percentage for all unicast data frames. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. The chart is updated approximately every 10 minutes. Right-click and select *Show Details* to view the Loss% details.

Airtime Utilization Chart

The *Airtime Utilization* chart displays station airtime utilization in percentage. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. The chart is updated approximately every 10 minutes. Right-click and select *Show Details* to view the *Airtime Utilization* details.

Station Information

The Station Information provides the *MAC Address*, *IPv4 Address*, *IPv6Address*, *User Name*, *Station Type*, *OUI Name*, *Device Type*, *OS Type*, *Radio Type*, *Data Rate*, *Service Name*, *Authentication*, *AP ID*, *AP Name*, and *Controller* details of the selected station.

802.11 Session

The *802.11 Session* is available for controller version 5.2 and higher versions. Each 802.11 Session is generated by events such as association, disassociation and hand offs. The 802.11 Session table provides the details of the Session duration and bytes transmitted during session. The 802.11 session details can be viewed in CSV format (comma separated values.) by selecting the CSV option.

Station History

The history of events accomplished through *FortiWLM* for the selected station along with the *Date/Time*, *Duration*, *Controller*, *AP ID*, *AP Name*, *Radio*, *Station IP4*, *Station IPv6*, *User Name*, *BSSID*, *L2 State* and *L3 State* events for the selected station can be viewed in this section. The Heat maps with the actual AP statistics retrieved from the controller is viewed by

selecting the *Go to Visualization* option. The station history can be viewed in CSV format (comma separated values) by selecting the CSV option.



The station history contains the complete history of sessions recorded for the chosen station in the station dashboard. This data is **not limited** to the time-range selected in the dashboard.

Station Activity Log

The *Station Activity Log* on the *Station Trend Dashboard* screen represents the station events only for the selected station. It displays the most recent 10,000 station events within the interval of one week. Once the number reaches 10,000, additional events are not listed. If additional events are important for troubleshooting, refine the time interval.

Most station events are updated almost immediately after the event occurs. All events are available on the server; to view other events, refine the time interval. The events can be filtered based on the event type. The station history can be viewed and exported in CSV format (comma separated values) by selecting the CSV option. The event types are filtered based on the station event type.

Figure 35 on page 85 illustrates the *Station Activity Log* screen.

Station Activity Log

Monitor > Station Activity > Station Activity Log

The *Station Activity Log* represents the station events of all stations within the selected time interval. Most station events are updated almost immediately after the event occurs. All events are available on the server; to view other events, refine the time interval. The station history can be viewed and exported in CSV format (comma separated values) by selecting the CSV option. The event types are filtered by selecting the controller, event severity, event Id, and MAC address.

Figure 35: Station Activity Log

Station Activity Log (325) Auto Refresh: 60 Sec

Filter Station Activity Log START TIME 11/22/2013 11:34:27 END TIME 11/22/2013 12:34:27 1-325 of 325 CSV

DATE/TIME	CONTROLLER	MAC ADDRESS	EVENT ID	SEVERITY	DESCRIPTION
2013-11-22 12:34:13.228193	172.19.43.251	94:39:e5:19:bac8	DHCP	Information	<msg_type=ACK><server_ip=172.19.43.1><server_mac=00:21:cc:5c:f1:a2><offered_ip=172.19.43.35>
2013-11-22 12:34:11.940193	172.19.43.251	94:39:e5:19:bac8	DHCP	Information	<msg_type=REQUEST><server_ip=255.255.255.255><server_mac=ff:ff:ff:ff:ff:ff><client_ip=0.0.0.0>
2013-11-22 12:34:11.910193	172.19.43.251	94:39:e5:19:bac8	802.1x Auth	Information	M4 <pkt type=EAPOL_KEY> <key type=Unicast Key> Key Pairwise
2013-11-22 12:34:11.833193	172.19.43.251	94:39:e5:19:bac8	802.1x Auth	Information	M3 <msg type=EAPOL_KEY> WPA2 PTK Negotiation sent
2013-11-22 12:34:11.833193	172.19.43.251	94:39:e5:19:bac8	802.1x Auth	Information	M2 <pkt type=EAPOL_KEY> MIC Verified
2013-11-22 12:34:11.527193	172.19.43.251	94:39:e5:19:bac8	802.1x Auth	Information	M1 <msg type=EAPOL_KEY> PTK sent
2013-11-22 12:34:11.526193	172.19.43.251	94:39:e5:19:bac8	802.11 State	Information	state change <old=Associated><new=Associated><AP=00:9c:e6:0c:f0:8f><BSSID=00:9c:e6:02:ea:69>
2013-11-22 12:34:11.097193	172.19.43.251	94:39:e5:19:bac8	802.11 State	Information	state change <old=Unauthenticated><new=Authenticated><AP=00:9c:e6:0c:f0:34><BSSID=00:9c:e6:02:dd:07>
2013-11-22 12:33:49.244193	172.19.43.251	94:39:e5:19:bac8	802.11 State	Information	Disassoc reason: Unspecified<AID=0><BSSID=00:9c:e6:02:dd:07>
2013-11-22 12:32:44.550193	172.19.43.251	94:39:e5:19:bac8	DHCP	Information	<msg_type=ACK><server_ip=172.19.43.1><server_mac=00:21:cc:5c:f1:a2><offered_ip=172.19.43.35>



The *Station Activity Log* was called as *Event Viewer*, prior to the 4.0-6-0 release.

See the **Station Activity Log** screen (*Monitor > Station Activity > Station Activity Log*) in Online Help for the Station Log details.

Tools

The *Tools* menu provides a *Search* and *Topology* options. The *Search* function allows you to explore for keywords appearing in data for *Reports*, *Inventory*, *Alarms*, *Configuration*, and/or *Stations*, including partial keyword search and advanced event filtering. The *Topology* provides at-a-glance system information and the logical placements of the hardware devices.

- “[Search Functionality](#)” on page 85
- “[Station Topology](#)” on page 90

Search Functionality

Monitor > Tools > Search

The search function is available on top of all windows and screens. You can use the search function to search for inventory, alarms, events, configuration profiles, and stations that are a part of your E(z)RF Application Suite. You can enter a keyword to search across all categories

or you can narrow your search results by selecting appropriate filters as listed in the following table.

Filters	Descriptions and Options	Search Output
Inventory	<p>You can search for all inventories that are currently connected or part of your E(z)RF deployment. Inventories are controllers and access points.</p> <p>To search for a controller or an access point, check the inventory option, type a keyword in the search text box, and select the <i>Search</i> option.</p>	<p>You can view a list of controllers with access points mapped to the selected controller that are connected to <i>FortiWLM</i> with the following details:</p> <ul style="list-style-type: none">• Controllers: The following controller details are displayed Controller Name, IP Address, Description, MAC Address, Model, Software Version, Availability Status, Administrative State, Location, and Controller Group.• Access Points: The following access points details are displayed: AP ID, AP Name, MAC Address, H/W model, Software Version, IP Address, Connectivity Preference, Location, Building, Controller, Availability Status, and AP Group.

Filters	Descriptions and Options	Search Output
		<ul style="list-style-type: none"> You are allowed to navigate to the following screens, to view the controller or the controller mapped to the access point: <ul style="list-style-type: none"> Connect (Connects to the controller) Inventory Details (Navigates to the <i>Controllers</i> screen in <i>Inventory > Devices > Controllers</i>) View Controller Dashboard (Navigates to the <i>Controller Dashboard</i> screen in <i>Monitor > Device Dashboard > Controller</i>) Inventory Details (Navigates to the <i>Access Points</i> screen in <i>Inventory > Devices > Access Points</i>) Topology (Navigates to the <i>Topology</i> screen in <i>Monitor > Tools > Topology</i>) View AP Dashboard (Navigates to the <i>AP Dashboard</i> screen in <i>Monitor > Device Dashboard > AP</i>) View Map Location (Navigates to the <i>AP Locator</i> screen in <i>Visualization > Heat Maps</i>)
Alarms	<p>You can search for all alarms that are notified by <i>FortiWLM</i>.</p> <p>To search for an alarm, check the alarm option, type a keyword in the search text box, and select the <i>Search</i> option. Narrow your search results by searching with <i>Active Alarms</i> or <i>History Alarms</i>.</p>	<p>You can view a list of alarms on FDN, notified by the <i>FortiWLM</i> with the following alarm details:</p> <p>FDN, Controller, Source, Alarm Name, Severity, Description, and Raised At.</p> <p>You are allowed to navigate to the Fault Management screen (<i>Monitor > Fault Dashboard > Fault Management</i>) by selecting the View alarms link.</p>

Filters	Descriptions and Options	Search Output
Events	<p>You can search for all events that occur on the <i>E(z)RF Network Manger</i>.</p> <p>To search for an event, check the events option, type a keyword in the search text box, and select the <i>Search</i> option.</p>	<p>You can view a list of events that occur in <i>FortiWLM</i> with the following event details:</p> <p>Event Name, Severity, Source, FDN, Controller, Generated At, Description, Authentication Type, and Reason.</p>
Configuration	<p>You can search for all types wireless service profiles or individual profiles, users and user groups that are currently connected or part of your <i>FortiWLM</i>.</p> <p>Configuration includes <i>Profiles</i> and <i>Administration</i>.</p> <p>To search for a wireless service profiles or individual profiles, users and user groups, check the configuration option, type a keyword in the search text box, and select the <i>Search</i> option.</p>	<ul style="list-style-type: none"> • Profiles: <ul style="list-style-type: none"> • You can view a list of wireless service profiles or individual profiles (ESS, Security, GRE, VLAN, RADIUS, RADIO, and Connectivity) with the respective SSID's and L2 Modes Allowed. • You are allowed to navigate and view the respective wireless service profiles or individual profiles (ESS, Security, GRE, VLAN, RADIUS, RADIO, and Connectivity) by selecting the <i>View</i> link. • Users and User Groups: <ul style="list-style-type: none"> • You can view a list of Users and User Groups with the following user details: User ID, User Name, User Group Id, User Description, Email Address, and Contact Details. • You can navigate to the User screen (<i>Administration > User Administration > Users</i>) or the User Groups screen (<i>Administration > User Administration > User Groups</i>) by selecting the <i>View Users</i> and <i>View User Groups</i> link.

Filters	Descriptions and Options	Search Output
Stations	<p>You can search for all stations connected to <i>FortiWLM</i>.</p> <p>To search for a station, check the stations option, type a keyword in the search text box, and select the <i>Search</i> option. Narrow your search results by searching with <i>Advanced Stations Filter</i>.</p>	<p>You can view a list of stations that are connected to <i>FortiWLM</i> with the following station details:</p> <p>MAC Address, AP ID, IPV4 Address, IPV6, BSSID, VLAN Name, ESS Name, User, Radio Type, and At Time.</p> <p>You are allowed to navigate to the Station Trend Dashboard screen (<i>Monitor > Station Activity > Station Dashboard</i>) by selecting the <i>View Station Dashboard</i> link.</p>

Figure 36 on page 89 illustrates the search engine.

Figure 36: Search

Search

Search

Filters:

☒ Inventory
☐ Alarms
☐ Events
☐ Configuration
☐ Stations

Keyword(s)

SEARCH

Enter search keyword(s) and click "Search" to continue.

See the **Search** screen (*Monitor > Tools > Search*) in Online Help for the details on search options.

Station Topology

Monitor > Tools > Topology

Topology is a tree that illustrates the logical placement of hardware devices. The hardware devices include *controllers*, *APs*, and *Stations*. Double-click *Stations* to see the following information for each client.

[Figure 37 on page 90](#) illustrates the *Station Topology* screen.

Figure 37: Station Topology

Topology																																																																							
NAVIGATION TREE		DETAILS: //ENTERPRISE/STATIONS																																																																					
<div>Enterprise</div> <div> <div>Controllers</div> <div>APs</div> <div>Stations</div> </div>		<div>Summary</div> <div>Total Stations 13</div>																																																																					
		<div>Station</div> <div>1 - 10 of 13</div> <table> <tr> <th>MAC ADDRESS</th><th>IP ADDRESS</th><th>CONTROLLER HOSTNAME</th><th>AP NAME</th><th>IF INDEX</th><th>BSSID</th></tr> <tr> <td>00:11:95:8b:9f:91</td><td>172.16.16.33</td><td>172.16.16.16</td><td>GF-QA320</td><td>2</td><td>00:0ce6:02:27:f8</td></tr> <tr> <td>00:21:5c:09:2c:41</td><td>172.16.17.14</td><td>172.16.16.16</td><td>IT-AP320</td><td>2</td><td>00:0ce6:02:7f:ac</td></tr> <tr> <td>00:21:6a:69:1a:30</td><td>172.16.17.13</td><td>172.16.16.16</td><td>GF-confAP320</td><td>2</td><td>00:0ce6:02:7f:ac</td></tr> <tr> <td>00:21:6a:89:89:b0</td><td>172.16.16.55</td><td>172.16.16.16</td><td>IT-AP320</td><td>2</td><td>00:0ce6:02:27:f8</td></tr> <tr> <td>00:22:43:19:49:6e</td><td>172.16.16.44</td><td>172.16.16.16</td><td>IT-AP320</td><td>2</td><td>00:0ce6:02:27:f8</td></tr> <tr> <td>00:90:0c:baccd:88</td><td>172.16.17.17</td><td>172.16.16.16</td><td>GF-QA320</td><td>1</td><td>00:0ce6:02:3e:42</td></tr> <tr> <td>3ca9:f4:18:54:80</td><td>172.16.16.12</td><td>172.16.16.16</td><td>IT-AP320</td><td>2</td><td>00:0ce6:02:27:f8</td></tr> <tr> <td>5c:59:48:11:a7:6c</td><td>172.16.16.25</td><td>172.16.16.16</td><td>IT-AP320</td><td>1</td><td>00:0ce6:02:bd:10</td></tr> <tr> <td>5c:f8:a1:2b:50:20</td><td>172.16.16.45</td><td>172.16.16.16</td><td>FF-QA-320</td><td>2</td><td>00:0ce6:02:27:f8</td></tr> <tr> <td>68:ed:43:65:e5:b7</td><td>0.0.0.0</td><td>172.16.16.16</td><td>GF-confAP320</td><td>1</td><td>00:0ce6:02:fe:f8</td></tr> </table>				MAC ADDRESS	IP ADDRESS	CONTROLLER HOSTNAME	AP NAME	IF INDEX	BSSID	00:11:95:8b:9f:91	172.16.16.33	172.16.16.16	GF-QA320	2	00:0ce6:02:27:f8	00:21:5c:09:2c:41	172.16.17.14	172.16.16.16	IT-AP320	2	00:0ce6:02:7f:ac	00:21:6a:69:1a:30	172.16.17.13	172.16.16.16	GF-confAP320	2	00:0ce6:02:7f:ac	00:21:6a:89:89:b0	172.16.16.55	172.16.16.16	IT-AP320	2	00:0ce6:02:27:f8	00:22:43:19:49:6e	172.16.16.44	172.16.16.16	IT-AP320	2	00:0ce6:02:27:f8	00:90:0c:baccd:88	172.16.17.17	172.16.16.16	GF-QA320	1	00:0ce6:02:3e:42	3ca9:f4:18:54:80	172.16.16.12	172.16.16.16	IT-AP320	2	00:0ce6:02:27:f8	5c:59:48:11:a7:6c	172.16.16.25	172.16.16.16	IT-AP320	1	00:0ce6:02:bd:10	5c:f8:a1:2b:50:20	172.16.16.45	172.16.16.16	FF-QA-320	2	00:0ce6:02:27:f8	68:ed:43:65:e5:b7	0.0.0.0	172.16.16.16	GF-confAP320	1	00:0ce6:02:fe:f8
MAC ADDRESS	IP ADDRESS	CONTROLLER HOSTNAME	AP NAME	IF INDEX	BSSID																																																																		
00:11:95:8b:9f:91	172.16.16.33	172.16.16.16	GF-QA320	2	00:0ce6:02:27:f8																																																																		
00:21:5c:09:2c:41	172.16.17.14	172.16.16.16	IT-AP320	2	00:0ce6:02:7f:ac																																																																		
00:21:6a:69:1a:30	172.16.17.13	172.16.16.16	GF-confAP320	2	00:0ce6:02:7f:ac																																																																		
00:21:6a:89:89:b0	172.16.16.55	172.16.16.16	IT-AP320	2	00:0ce6:02:27:f8																																																																		
00:22:43:19:49:6e	172.16.16.44	172.16.16.16	IT-AP320	2	00:0ce6:02:27:f8																																																																		
00:90:0c:baccd:88	172.16.17.17	172.16.16.16	GF-QA320	1	00:0ce6:02:3e:42																																																																		
3ca9:f4:18:54:80	172.16.16.12	172.16.16.16	IT-AP320	2	00:0ce6:02:27:f8																																																																		
5c:59:48:11:a7:6c	172.16.16.25	172.16.16.16	IT-AP320	1	00:0ce6:02:bd:10																																																																		
5c:f8:a1:2b:50:20	172.16.16.45	172.16.16.16	FF-QA-320	2	00:0ce6:02:27:f8																																																																		
68:ed:43:65:e5:b7	0.0.0.0	172.16.16.16	GF-confAP320	1	00:0ce6:02:fe:f8																																																																		

Controllers

Select *Controllers* from the tree. The following sections are displayed:

Figure 38: Station Topology - Controllers

Topology

NAVIGATION TREE

Clear Tree

Enterprise

Controllers

APs

Stations

DETAILS: //ENTERPRISE/CONTROLLERS

Summary

Total Controllers

1

Controllers

1 - 1 of 1

HOSTNAME	IP ADDRESS	STATUS	SERIAL #	UPTIME	H/W PLATFORM	S/W VERSION	LOCATION	DESCRIPTION	CONTROLLER UI
172.16.16.16	172.16.16.16	Online	00:90:0b:1a:f0:93	02d:20h:31m:04s	MC4200	5.3-155		controller	Go to Controller

- **Summary:** Displays the total number of controllers. [Figure 38 on page 90](#) illustrates the *Controllers Station Topology*.

- **Controllers:** Displays the list of controllers managed by *FortiWLM* in a tabular format. The controllers table provides the following details:

Field	Description
Hostname	Displays the controller's Hostname or IP Address. Select the hyper link of the controller's IP address. The selected controller's IP address gets included to the controllers tree.
IP Address	Displays the controller's IP Address.
Status	Displays the controller's status whether Online or Offline.
Serial#	Displays the serial number of the controller.
Uptime	Displays the controller's uptime.
H/W Platform	Displays the hardware platform associated to the controller.
S/W Version	Displays the software version of the controller.
Location	Displays the location of the controller.
Description	Displays the description provided for the controller.
Controller UI	Select the hyper link of the controller, the selected controller is displayed.

Access Points

Select the APs from the tree. The following sections are displayed:

Figure 39 on page 91 illustrates the *APs Station Topology* screen.

Figure 39: Station Topology - APs

Topology

Topology

NAVIGATION TREE

Clear Tree

DETAILS: //ENTERPRISE/APs

Enterprise

Controllers

APs

Stations

Summary

Total APs8

AP

<< < 1 - 8 of 8 > >

AP NAME	AP ID	IP ADDRESS	STATUS	SERIAL #	CONTROLLER HOSTNAME	MAP LOCATION	AP MODEL	S/W VERSION
AP-13	13	172.18.114.11	Online	00:0ce6:60:ceb:e9	172.19.43.251	Enterprise >> Campus_1 >> Building_1 >> Floor_2	AP1010	6.0-8-0
AP-9	9	172.19.32.127	Online	00:0ce6:60:cef:7a	172.19.43.251	Enterprise >> Campus_1 >> Building_1 >> Floor_2	AP1010	6.0-8-0
AP-4	4	172.19.32.121	Online	00:0ce6:60:c:f9:34	172.19.43.251	Enterprise >> Campus_1 >> Building_1 >> Floor_2	AP1010	6.0-8-0
AP-8	8	172.19.32.116	Online	00:0ce6:60:c:f9:50	172.19.43.251	Enterprise >> Campus_1 >> Building_1 >> Floor_2	AP1010	6.0-8-0
AP-1	1	172.19.32.196	Online	00:0ce6:60:c:f9:8f	172.19.43.251	Enterprise >> Campus_1 >> Building_1 >> Floor_2	AP1010	6.0-8-0
AP-2	2	172.19.32.160	Online	00:0ce6:60:dbef:1f	172.19.43.227	Enterprise >> Campus_1 >> Building_1 >> Floor_1	AP332i	5.3-149-1
AP-1	1	172.19.32.43	Online	00:0ce6:60:df:d7	172.19.43.227	Enterprise >> Campus_1 >> Building_1 >> Floor_1	AP332e	5.3-149-1
AP-11	11	172.19.0.132	Online	00:0ce6:11:25:d5	172.19.43.251	Enterprise >> Campus_1 >> Building_1 >> Floor_2	AP832e	6.0-8-0

Summary: Displays the details of the selected AP managed by *FortiWLM* in a tabular format. The AP table provides the following details:

Field	Description
AP Name	Displays the <i>AP Name</i> . Select the hyper link of the <i>AP Name</i> . The selected AP name address gets included to the AP tree.
AP ID	Displays the <i>AP ID</i> to which the station was associated at the time of the event.
IP Address	Displays the controller's IP Address. Note: For APs connected through L2 to a controller, the IP address displayed is 0.0.0.0 For Teton APs, the information for three radios are displayed.
Status	Displays the AP status whether <i>Online</i> or <i>Offline</i> .
Serial#	Displays the serial number of the AP.
Controller Hostname	Displays the controller's Hostname.
Map Location	Displays the <i>Map Location</i> . Select the hyper link of the map location. The <i>Map Management</i> screen is displayed.
AP Model	Displays the AP Model.
S/W Version	Displays the software version of the AP.

Interface: The Interface table provides the following details:

Field	Description
IF Index	Displays the Interface Index number. <ul style="list-style-type: none"> • Select the hyper link of the Interface Index. • The selected Interface is added to the Interface tree. • A summary of the Interface Index is displayed, depicting the stations connected to the selected Interface.
Serial#	Displays the Serial number of the AP.
AP Name	Displays the AP Name.
Channel	Displays the Channel number.

Stations

Select the *Stations* from the tree. The following sections are displayed:

Summary: Displays the total number of stations.

Figure 40 on page 93 illustrates the *Station Topology* screen.

Figure 40: *Station Topology*

Topology

Topology

NAVIGATION TREE

Clear Tree

Enterprise

Controllers

APs

Stations

DETAILS: //ENTERPRISE/STATIONS

Summary

Total Stations

3

Station

<< 1 - 3 of 3 >>

MAC ADDRESS	IP ADDRESS	CONTROLLER HOSTNAME	AP NAME	IF INDEX	BSSID
3c:a9:f4:18:55:a4	172.19.43.27	172.19.43.251	AP-9	1	00:0c:e6:02:6c:91
7c:e9:d3:f7:7b:f6	172.19.43.33	172.19.43.251	AP-13	1	00:0c:e6:02:77:2b
94:39:e5:19:bac:8	172.19.43.35	172.19.43.251	AP-1	1	00:0c:e6:02:ea:69

Station: Displays the list of *Stations* managed by *FortiWLM* in a tabular format. The Station table provides the following details:

Field	Description
MAC Address	Displays the station <i>MAC Address</i> . Select the hyper link of the MAC Address. The selected <i>MAC Address</i> gets included to the station's tree.
IP Address	Displays the controller's IP address.
Controller Hostname	Displays the controller's hostname.
AP Name	Displays the AP name.
IF Index	Displays the IF index.
BSSID	Displays the BSSID of the associated station.

FortiWLM Status Bar

The *FortiWLM* icons displayed on the *Status bar* are refreshed every 60 seconds to provide global information of the managed network. The following Icons are displayed on the status bar:

Icons	Description
Alarms	<p>The <i>Alarms</i> frame on the status bar displays the following alarm icons along with the count of active alarms in brackets. Hovering the mouse cursor over the alarms frame displays a table of the respective alarms by severity and count.</p> <ul style="list-style-type: none">• Critical Alarms<ul style="list-style-type: none">• Critical Alarms are represented by <i>red</i> color and indicates the need for immediate action.• Typical critical alarms are generated either when a controller or AP is down, or when a rogue AP is detected. The <i>Rogue</i> alarm is raised when the <i>Wired Rogue</i> is detected.• Major Alarms<ul style="list-style-type: none">• Major Alarms are represented by <i>orange</i> color and indicates the need for action when ever required.• Typical major alarms are displayed due to <i>Authentication failure</i>.• Minor Alarms<ul style="list-style-type: none">• Minor Alarms are represented by <i>yellow</i> color and does not require any action.• Typical minor alarms are displayed due to MIC errors. <p>The detailed list of <i>Alarms</i> is also available on the <i>Alarms</i> screen of the Fault Management screen.</p>

Icons	Description
Controllers	<p>The <i>Controllers</i> frame on the <i>Status Bar</i> displays the following <i>Controller</i> icons along with the count of active controllers in brackets, which indicates whether a controller is reachable from FortiWLM or not. Hovering the mouse cursor over the controllers frame displays a table of the respective controller in detail.</p> <ul style="list-style-type: none"> • Online Controllers indicates reachable. • Offline Controllers indicates not-reachable. • Unmanaged indicates not managed by FortiWLM. <p>The detailed information on <i>Controllers</i> is also available on the <i>Controllers</i> screen.</p>
APs	<p>The <i>APs</i> frame on the <i>Status Bar</i> displays the following AP icons along with the count of APs present on the managed controller. Hovering the cursor over the APs frame displays a table of the respective AP in detail.</p> <ul style="list-style-type: none"> • Online indicates the availability of APs in <i>Online</i> state on the managed controller. • Offline indicates the availability of APs in <i>Offline</i> state on the managed controller. • Unknown indicates the availability of APs in <i>Unknown</i> state on the managed controller. <p>The detailed information on APs is also available on the <i>Access Points</i> screen.</p> <ul style="list-style-type: none"> • Mismatched APs: This provides a list of APs with the configuration mismatch displayed along with the time stamp when the mismatch was detected. <p>The detailed information on <i>Mismatched APs</i> is also available on the <i>APs Not In Sync With NMS Configuration</i> screen.</p>

Icons	Description
Rogue	<p>The <i>Rogue</i> frame on the Status Bar displays the following Rogue icons along with the count of Rouges present on the managed controller. Hovering the cursor over the Rogue frame displays a table of the respective Rogue in detail.</p> <ul style="list-style-type: none"> • Rogue APs indicates all the wireless rogue APs present on the managed controller. • Wired Rogue APs indicates all the wired rogue APs present on the managed controller. This alarm is raised when the when the Wired Rogue is detected. <p>The detailed information on <i>Rogues</i> is also available on the <i>Alarms</i> screen.</p>
Stations	<p>The Stations frame on the Status Bar displays the following Station icons along with the count of Stations present on the managed controller. Hovering the cursor over the Station frame displays a table of the respective Station in detail.</p> <ul style="list-style-type: none"> • <i>Stations</i> indicate all the stations present on the managed controller. • <i>Phones</i> indicate all the stations present on the managed controller. <p>The detailed information on <i>Stations</i> is also available on the <i>Station Trend Dashboard</i>.</p>
Resources	<p>The <i>Resources</i> frame on the Status Bar displays the Memory Usage and the CPU Usage details.</p>
Uptime	<p>Displays the amount of time the controller has been up (in days:hours:minutes:seconds format).</p>

4 Configuring FortiWLM

You can use *FortiWLM* to manage multiple *FortiWLC*. One of the major features of *NM* is the ability to create a controller configuration from *FortiWLM* and download it to one or more managed controllers. These controller configurations are owned by the *nms* - server and cannot be altered by the controllers using them.

This chapter describes creating and applying controller configurations.

The *NM* can download the controller configuration to one or all managed controllers. If you modify the controller configuration, all controllers using it are automatically updated with those modifications. The configuration of controllers is managed by *FortiWLM* via a *Wireless Service Profile*, *AP Template*, and *Service Control*.

- [“Profiles” on page 97](#)
- [“Templates” on page 148](#)
- [“Controller Configuration” on page 169](#)

Profiles

FortiWLM allows you to create a common configuration for multiple controllers. A controller configuration comprising of multiple profiles (*ESS Profile*, *Security Profile*, *RADIUS Profile*, and *Tunnel (GRE/VLAN) Profile*) is created and downloaded to one or more managed controllers or *AP Groups*. These multiple profiles support a wide variety of connection requirements which enhances the wireless security.

- Service Profile - [“Add a Service Profile in FortiWLM” on page 99](#)
- ESS Profile - [“ESS Profile in FortiWLM” on page 107](#)
- Security Profile - [“Security Profile in FortiWLM” on page 113](#)
- RADIUS Profile - [“RADIUS Profile” on page 118](#)
- VLAN Profile - [“VLAN Profile in FortiWLM” on page 130](#)
- GRE Profile - [“GRE Profile in FortiWLM” on page 140](#)

Wireless Service Profiles

A wireless service profile is a set of configurations created on the *NM* server that is applied to a controller to create the service on the controller. A service profile consists of *ESS Profile*, *Security Profile*, *RADIUS Profile*, and *Tunnel (GRE/VLAN) Profile*. The ESS and security profiles are common across multiple controllers, the *RADIUS Profiles* can be common or controller specific and the *Tunnel Profiles* are configured per controller basis.

All complete service profiles are registered to controllers or AP groups. A service profile is said to be *complete* only if the configurations for the required fields in the profile with the dependent configuration profiles are complete and the profile is effective on saving or registering on to the controller. The service profile is said to be *incomplete* if the configurations for the required fields in the profile along with the dependent configuration profiles are incomplete. Incomplete service profiles will not be registered to a controller but will be saved in the database. The incomplete profile can be completed by providing the input data for all the missing fields and then can be registered to a controller or an AP Group.

While selecting a profile you can select one of the existing profiles that were individually created (*Configuration > Profiles > ESS, Security, RADIUS, VLAN or GRE*) or provide a name of the non-existent profile and create the named profile at later point of time. Once the named profile is created, the service profile is applied to the registered controllers.

Add a Service Profile in FortiWLM

1. Navigate to *Configuration > Templates > Wireless Service*.
2. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.

Figure 41 on page 100 illustrates the *Service Profile - Add* screen.

Figure 41: Service Profile - Add

Service Profile - Add

Name *	<input type="text"/>	[1-32] chars.,
Description	<input type="text"/>	[0-128] chars.
ESS Profile *	<input type="text"/>	[1-32] chars.,
ESS Profile for Overflow	<input type="text"/>	[0-32] chars.
Security Profile *	<input type="text"/>	[1-32] chars.,
Primary Authentication RADIUS	<input type="text"/>	[0-16] chars.
Secondary Authentication RADIUS	<input type="text"/>	[0-16] chars.
Primary Accounting RADIUS	<input type="text"/>	[0-16] chars.
Secondary Accounting RADIUS	<input type="text"/>	[0-16] chars.
Primary MAC AUTH RADIUS	<input type="text"/>	[0-16] chars.
Secondary MAC AUTH RADIUS	<input type="text"/>	[0-16] chars.
Primary MAC Accounting RADIUS	<input type="text"/>	[0-16] chars.
Secondary MAC Accounting RADIUS	<input type="text"/>	[0-16] chars.
Tunnel Interface Type	<input type="text" value="No Tunnel"/>	
VLAN Profile	<input type="text"/>	[0-32] chars.
GRE Profile	<input type="text"/>	[0-32] chars.
VLAN Pool Profile	<input type="text"/>	[0-32] chars.
TIMER Profile	<input type="text"/>	[0-32] chars.
Backup ESS Profile	<input type="text"/>	[0-32] chars.
Backup Security Profile	<input type="text"/>	[0-32] chars.
Hotspot Profile	<input type="text"/>	[0-16] chars.

- In the *Service Profile* screen, select *Add or Plus* icon.
- The *Service Profile - Add* screen allows you to select existing *ESS Profile*, *Security Profile*, *RADIUS Profile*, and *Tunnel (GRE/VLAN) Profile* to associate with the service profile. By default, the service profile is associated with the ESS and security profiles named default.

5. In the *Name* field, type the name of the service profile. The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
6. In the *Description* field, provide a description for the service profile. The description can be up to 128 characters long and can contain spaces and special characters (for example, Service Profile - ESS Profile).
7. In the *ESS Profile* field, type a new ESS profile name or select an existing ESS profile from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
Configuration > Templates > Wireless Service > Service Profile > ESS Profile
Configuration > Profiles > ESS > Select a ESS Profile > Edit option
 The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
8. In the *ESS Profile for Overflow* field, type the ESS profile for overflow name or select an existing ESS profile for overflow from the drop-down list. This field is applicable for all AP300 or AP400 model. This works by having the two ESS profiles share an SSID so they can seamlessly move clients back and forth as needed.
9. In the *Security Profile* field, type the security profile name or select an existing security profile from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
Configuration > Templates > Wireless Service > Service Profile > Security Profile
Configuration > Profiles > Security > Select a Security Profile > Edit option
 The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
 ESS profiles and Security profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Wireless > Configuration > ESS* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
10. The *RADIUS* is AAA protocol (authentication, authorization and accounting) server that comprises of the user names and passwords of all the users to authenticate a client. *RADIUS Profiles* can be either common to all controllers or specific to one controller.
 - *Common RADIUS profiles* are created by navigating to,
Configuration > Templates > Wireless Service > Choose a Service Profile > Select Edit option > Service Profile - Update screen.
 In the *Primary Authentication Radius* field, type the data for the following fields to create common RADIUS profiles.
 - Primary Authentication
 - Secondary Authentication
 - Primary Accounting
 - Secondary Accounting
 - Primary MAC AUTH RADIUS

- Secondary MAC AUTH RADIUS
The above names can be up to 16 alphanumeric characters long with no spaces. This is an optional field.
 - *Controller specific RADIUS profiles* are created by navigating to,
 - *Configuration > Templates > Wireless Service > Choose a Service Profile > Select Edit option > Service Profile - Update screen > Choose the Radius Profile tab > Select Primary Authentication tab > Select the Add or plus icon to add Individual Controller Radius Configuration.*
 - *Configuration > Profiles > Radius > Radius Profile screen > Select the Add or plus icon to add Individual Controller Radius Configuration.* Controller specific RADIUS profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Wireless > Configuration > Security > RADIUS* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
11. In the *Tunnel Interface Type*, select a tunnel interface type from the drop-down list. The following are the options:
- *No Tunnel*: No tunnel is associated with this service profile.
 - *Configured VLAN Only*: A configured VLAN only is listed in the following VLAN Name list is associated with this service profile.
 - *Radius VLAN Only*: The VLAN is assigned by the RADIUS server via the RADIUS attribute Tunnel Id. Use RADIUS VLAN Only when clients authenticate via 802.1x/WPA/WPA2 or MAC Filtering.
 - *Radius and Configured VLAN*: Both configured VLAN and RADIUS VLAN are associated with this service profile.
 - *GRE*: Specifies a GRE Tunnel configuration.

This is an optional field.

12. If you have selected the *Tunnel Interface Type* as *Configured VLAN Only*, *Radius VLAN Only*, and *Radius and Configured VLAN*, type a *VLAN Profile* name or select an existing *VLAN Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
Configuration > Templates > Wireless Service > Service Profile > Edit > Service Profile - Update > VLAN Profile
Configuration > Profiles > VLAN > Add
 The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
13. If you have selected the *Tunnel Interface Type* as *GRE*, type a *GRE Profile* name or select an existing *GRE Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
Configuration > Templates > Wireless Service > Service Profile > GRE Profile
Configuration > Profiles > GRE > Add



14. Complete the *Service Profile* and select *Save* option. The service profile with the set of *ESS Profile*, *Security Profile*, *RADIUS*, and *Tunnel Profiles (GRE/VLAN)* are displayed on the *Service Profile* screen.

The ESS profile and security profile are default profiles across multiple controllers where as the *RADIUS and Tunnel Profiles (GRE/VLAN)* are configured per controller basis.

You can now clone a wireless service profile instead of creating a duplicate manually. All profiles (except VLAN and GRE) in the service profiles is cloned. For detailed information, see the online help for Service Profile.

Complete the Registration of a Service Profile in FortiWLM

To complete the registration of a service profile, follow the below steps:

- 103

3. Select a check box of the *Service Profile* and select *Edit*. [Figure 42 on page 105](#) illustrates the *Service Profile - Registration* screen.
The following tabs are displayed:
 - Service Profile
 - Registration
 - ESS Profile
 - Security Profile
4. Select the *Registration* tab. The *Service Profile - Registration* screen displays a list of controllers and AP groups registered to that particular service profile. The *Service Profile - Registration* screen provides the following details:
 - *Registered Member*: Displays the host name or IP address of the registered member.
 - *Member Type*: Displays if the member type is a controller or AP group.
 - *Auto-Sync*: Displays if the Auto-Sync is *On* or *Off*.
 - *Last Sync Time*: Displays the last sync time of the service profile to the registered controller or an AP group.
 - *Sync Status*: Displays the sync status of the service profile to the registered controller or an AP group. The following are the types:
 - *In-Sync*: The service profile status is displayed as *In-Sync* for the profiles with *Auto-sync* as *On* and are successfully applied to all APs or Controllers.
 - *Sync Pending*: All the incomplete service profiles display the Status as *Sync-Pending*.
 - *Failed*: The service profile status is displayed as *Failed* if the controllers are in the *Deleted* or the controllers are *not managed* or the controllers are in the *Unlicensed* state. If the controller registered to the service profile is unregistered, all the profiles on that controller belonging to the service profile is deleted from the *Registration* table. [Figure 42 on page 105](#) illustrates the *Service Profile - Registration* screen.
 - *Sync Details*: Displays the reason for the controller or AP group that failed to sync.
 - *Controller Group Name*: The Controller group the Service profile is registered to.

- Nodename: The name of the Controller.

Figure 42: Service Profile - Registration



Slave controllers cannot be registered to a service profile. The status is displayed as *Sync Failed* when registered to a slave controller.

You will be able to perform the following actions on the *Service Profile - Registration* screen:

- **Auto-Sync:**
 - Select the *Edit* option for a Controller or an AP Group.
 - Select the *Auto-Sync* to *On* in the Registration-Update screen. The option *On* enables the service profile to synchronize any modified data to the registered controller or an AP group. If any of the profiles within the *Service Profile* is modified, the modified profile is automatically synchronized to the registered controller only when the *Auto-sync* is set to *On*.
- **Register:** Select the service profile and register to a controller, AP, or an AP Group.
- **Unregister:** Select controllers or AP groups check box and select the *Unregister* option. The following are the scenarios:
 - Unregistering a service from the AP group deletes the services from all the APs within the group.
 - When the service is registered to both AP group and controllers, by unregistering a service from the controller will delete the services only on the APs which are not part of the registered AP group.
 - If the controller is not online at the time of service un-registration, the services will be unregistered for the APs after the controller comes online.
 - All the service profiles get unregistered from the AP group, when an AP Group is deleted.
 - When a service profile is deleted, the services will be unregistered from all the APs within the AP group to which the service is registered.
 - When the controller is deleted from the inventory, the APs corresponding to the controller will not be deleted from the AP group. But the services will be deleted on those APs.
- **Force Sync:** You can perform the necessary modifications on failed APs and allow to perform a *Force Sync*.

See the **Service Profile - Registration** screen (*Configuration > Templates > Wireless Service > Edit*) in Online Help for detailed information on *Service Profile - Registration* topic.

Verify if a Controller is using NM or a Controller Configuration

There are three options to determine whether a controller is using a *FortiWLM* configuration or Controller configuration.

The first option to determine which controllers are using a service profile in the *FortiWLM* is by following these steps:

1. Navigate to *Configuration > Templates > Wireless Service*. The *Service Profile* screen provides a list of service profiles to which a controller or an AP group can be registered.
2. Choose a *Service Profile* and select *Edit*. The following tabs are displayed:
 - Service Profile
 - Registration
 - ESS Profile
 - Security Profile
3. Select the *Registration* tab, the *Service Profile - Registration* screen provides a list of controllers and AP groups registered to the Service Profiles.
4. The "Member Type" column of the *Service Profile - Registration* screen displays if the service profile is registered to controllers or AP groups. [Figure 42 on page 105](#) illustrates the *Service Profile - Registration* screen.

The second option to determine which controllers are using a service profile in *FortiWLM* is to view a controller's current profiles by following these steps:

1. Navigate to *Configuration > Device View > Controllers Configuration*. The *Controllers View* screen displays a list of controllers to which the profiles are applied.
2. Choose a controller from the *Controllers View* screen and select *View*.
3. The *Controller View* tab with each profile tab (*ESS Profile*, *Security Profile*, *RADIUS Profile*, *VLAN Profile*, and *GRE Profile*) is displayed. The profiles applied on the controller from *FortiWLM* are indicated here.



You cannot perform any modifications from here.

The third option to determine the controller configuration is by viewing the controller (SD) itself. From the controller, click *Wireless > Configuration > ESS* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.

ESS Profile in FortiWLM

A basic service set (BSS) is the basic building block of an IEEE 802.11 wireless LAN; one access point together with all associated clients is called a BSS. The BSSs can create coverage in small offices and homes, but they cannot provide network coverage to larger areas. 802.11 allows wireless networks of arbitrarily large size to be created by linking BSSs into an extended service set (ESS). An ESS is created by chaining BSSs together with a backbone network. An AP acquires its clients by broadcasting its name (SSID) which is picked up by clients within range. Clients can then respond, establishing a connection. It is legitimate for multiple access points to share the same SSID if they provide access to the same network as part of an Extended Service Set (ESS).

The ESS profiles can be configured either from FortiWLM or from the controller. To add an ESS from the *NM* web UI, follow these steps:

1. Navigate to *Configuration > Templates > Wireless Service*. The *Service Profile* screen displays a list of Service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit*. The following tabs are displayed:
 - Service Profile
 - Registration
 - ESS Profile
 - Security Profile
3. Select the *ESS Profile* tab, the *Service Profile - ESS Profile* screen is displayed. [Figure 43 on page 108](#) illustrates the *Service Profile - ESS Profile* screen.

Figure 43: Service Profile - ESS Profile

Service Profile: Scale_ServicePro_911

Service Profile

Registration

ESS Profile

Security Profile

VLAN Profile

ESS Profile Name

Scale_ESSPro_911

SSID

Scale_ESSPro_911

Enable/Disable

Enable

ESSID TYPE

Essid Type

Regular

Accounting Interim Interval (seconds)

3600

Valid range: [600-36000]

Reconnect Primary Server (minutes)

10

Valid range: [5-60]

Bridging

☐ IPV6

802.11r

Off

802.11r Group

7

Valid range: [1-65535]

802.11k

Off

DATAPLANE MODE

Dataplane Mode

Tunneled

AP VLAN Policy

No VLAN

AP VLAN Tag*

0

Valid range: [0-4094],

Enable AP VLAN Priority

Off

IP Prefix Validation

Off

VIRTUALIZATION MODE

RF Virtualization Mode

Virtual Port

ACM Support

☐ ACM Voice
☐ ACM Video

GENERAL SETTINGS

4. In the *Enable/Disable* drop-down list, select one of the following:
 - *Enable*: ESS Profile created is enabled.
 - *Disable*: ESS Profile created is Disabled.
5. In the *Accounting Interim Interval* field, type the time (in seconds) that elapses between accounting information updates for RADIUS authentication. If a RADIUS accounting server is enabled, the controller sends an interim accounting record to the RADIUS server at the interval specified. Accounting records are only sent to the RADIUS server for clients

that authenticate using 802.1x. The interval can be from 600 through 36,000 seconds (10 minutes through 10 hours). The default value is 3,600 seconds (1 hour).

6. Beacon Interval sets the rate at which beacons are transmitted. Setting the beacon interval to a higher value decreases the frequency of unicasts and broadcasts sent by the access point. If the power-save feature is enabled on clients that are connected to access points, clients “wake up” less if fewer unicasts and broadcasts are sent, which conserves the battery life for the clients. In the Beacon Interval field, type the interval (in ms) at which beacons are transmitted. The beacon interval must be between 20 through 1000 milliseconds. For AP300/AP400 and AP1000, beacon interval is a multiple of 20, from 20 to 1000ms. If your WLAN consists mostly of Wi-Fi phones, and you have a low number of ESSIDs configured (for example, one or two), Fortinet recommends setting the beacon interval to 100.
7. In the SSID Broadcast drop-down list, select one of the following:
 - *On*: SSID is included in the beacons transmitted.
 - *Off*: SSID is not included in the beacons transmitted. Also Probe Responses will not be sent in response to Probe Requests that do not specify an SSID.
 - *2.4GHz only*: SSID is included in the 2.4GHz beacons transmitted.
 - *5GHz only*: SSID is included in the 5GHz beacons transmitted.
8. In the Bridging area, verify any of these bridging options:
 - *AirFortress*: FortressTech Layer 2 bridging and encryption with Fortress Technology Air-Fortress gateway.
 - *IPv6*: Configures bridging Internet version 6 addresses. IPv6 via tunneling mode has these limitations:
 - No dynamic VLAN
 - No multiple ESSID mapping to same VLAN
 - No support for IPv6 filtering
 - No IPv6 IGMP snooping
 - *AppleTalk*: configures bridging to AppleTalk networks on this ESS.
9. By default, access points that join the ESS profile and have the same channel form a Virtual Cell. In the *New APs Join ESS* profile drop-down list, select one of the following:
 - *On*: (default) Access points automatically join an ESS profile and are configured with its parameters.
 - *Off*: Prevents access points from automatically joining an ESS profile. The user is now allowed to add multiple interfaces on the ESS Profile screen.
10. In the *Allow Multicast Flag* drop-down list, optionally enable multicasting (on). Only enable multicasting if you need to use a multicast application. Enabling multicasting causes all multicast packets on the air side to appear on the wired side, and all multicast packets on the wired side to appear on the air side.
Multicasting is a technique frequently used for the delivery of streaming media, such as video, to a group of destinations simultaneously. Instead of sending a copy of the stream

to each client, clients share one copy of the information, reducing the load on the network. Multicasting is an advanced feature and can cause subtle changes in your network. By default, multicasting is disabled and should be enabled only for specific circumstances.

- On: Enables multicasting. Enable multicasting only if you need to use a multicast application. Enabling multicasting causes all multicast packets on the air side to appear on the wired side, and all multicast packets on the wired side to appear on the air side.
- Off: Disables multicasting.



Multicasting is allowed only when an ESS profile has a one-to-one mapping with the default VLAN for this ESS profile; no other ESS profile uses the same VLAN; and security rules associated with this ESS profile do not redirect traffic to another VLAN. Multicasting is an advanced feature. Enabling multicasting in the Fortinet WLAN System can cause subtle changes in your network. Contact Fortinet Technical Support before enabling multicasting.

11. In the *Isolate Wireless to Wireless Traffic* drop-down list, optionally enable the Isolate wireless to wireless traffic (on). This is enabled to prevent two wireless stations operating on the same L2 domain from communicating directly with each other. This is not a common requirement, but can be necessary for some security policies. Set the option to On if your network requires this.
12. In the *Silent Client Polling* drop-down list, optionally enable the silent client polling (on).
 - On: Enables tracking information to be sent between the Controller and the APs and between the AP and a phone that is not in a call or during power save. This feature keeps the system apprised of a client phone location if the client moves between APs while the phone is inactive.
 - Off: Disables silent client polling.
13. In the *Multiple IP per Station* drop-down list, optionally enable the multiple IP per station (on).
14. In the Multicast-to-Unicast Conversion optionally enable the conversion (on) select one of the following:
 - On: Enables multicast-to-unicast conversion. Enabling this conversion allows multicast packets to be converted to unicast packets and deliver it all the clients.
 - Off: Disables multicast-to-unicast conversion. The multicast packets will be delivered as multicast packets to the clients.
15. In the *RF Virtualization Mode* drop-down list select the user to specify the type of virtualization used by the specified ESS profile. The option for selections are as follows:
 - *Virtual Cell*: This is the default setting for all APs except AP300 and AP400 models.
 - *Virtual Port*: This is the default setting for AP300 and AP400 models.
 - *Native Cell*: This option disables virtualization on the ESS.
16. In the *WMM Support* drop-down list, select one of the following:
 - On: Enables Wifi Multimedia (WMM) Enhanced Distribution Channel Access (EDCA) for QoS priority scheduling and Automatic Power Save Delivery (APSD) for improvements over the 802.11 legacy power management. WMM is on by default.

- *Off*: Disables WMM.
17. In the *APSD Support* drop-down list (*Advanced WMM Power Save*), select one of the following:
- *On*: Data packets for power save mode clients are buffered and delivered based on the trigger provided by the client. This feature saves more power and provides longer life-time for batteries than the legacy power save mode (TIM method).
 - *Off*: No U-APSD support
18. In the *DTIM Period* text box, type the number of beacon intervals that elapse before broadcast frames stored in buffers are sent. This value is transmitted in the DTIM period field of beacon frames. The DTIM period can be a value from 1 through 255. The default DTIM period is 1. Setting the DTIM period to a higher value decreases the frequency of broadcasts sent by the access point. If power save is enabled on clients that are connected to access points, clients "wake up" less if fewer broadcasts are sent, which conserves battery life for the clients. Only the behavior of clients currently in power-save mode is affected by the DTIM period value. Because broadcasts are generally wasteful of air resources, the Fortinet WLAN has devised some mechanisms that mitigate broadcasts either with proxy services or with more efficient, limited unicasts. As an example, ARP Layer 2 broadcasts received by the wired side are not relayed to all wireless clients. Instead, the Forti WLC maintains a list of IP-MAC address mappings for all wireless clients and replies with proxy-ARP on behalf of the client.
19. In the *Dataplane Mode* drop-down list, select the type of AP/Controller configuration:
- *Tunneled*: The default connection between controllers and APs, where data and control packets are passed.
 - *Bridged*: (formerly Remote AP mode) Bridged mode ESS profiles are supported by AP300s. In bridged mode, data packets are not passed to the controller; only control plane packets are passed to the controller. This setting determines the type of traffic that is passed between the controller and an AP. By default, tunneled mode is active where a controller and an AP are connected with a data tunnel so that data from a mobile station is tunneled to the controller from the AP and vice versa. When bridged mode is configured, an AP can be installed and managed at a location separated from the controller by a WAN or ISP, for example a satellite office. The controller monitors the remote APs through a keep-alive signal. Remote APs can exchange control information, including authentication and accounting information, with the controller but are unable to exchange data. Remote APs can exchange data with other APs within their subnet. Because remote APs cannot exchange dataplane traffic (including DHCP) with the controller, these System Director features are not available for Remote AP configuration: Virtual Cell, VLAN, Captive Portal, L3 Mobility, and QoS. A VLAN tag can be configured for a Bridged mode profile (see below) and then multiple profiles can be associated to that VLAN tag.
20. The *AP VLAN Policy* is selected for the *Bridged dataplane* mode. The following are the types of AP VLAN Policy that can be selected from the drop-down list.
- No VLAN

- Static VLAN
 - RADIUS VLAN Only
 - RADIUS and Static VLAN
- 21.** The AP VLAN Tag can be selected only if the *AP VLAN Policy* is selected as *Static VLAN* or *RADIUS and Static VLAN*. This VLAN tag value is configured in the controller's VLAN profile and is used for tagging client traffic (for the ESSIDs with dataplane mode bridged) using 802.1q VLAN. AP VLAN Tag is a number between zero and 4094. This is a mandatory field.
- 22.** In the *Enable APVLAN priority* drop-down list optionally set the Enable APVLAN priority on or off.
- *On*: AP disregards the DSCP value in the IP header of a packet.
 - *Off*: AP honors the DSCP values in the IP header of a packet. AP converts the DSCP value in the IP header to appropriate WMM queues. This feature works only for downstream packets and only for ESSID with dataplane mode as bridged.
- 23.** The Band steering mode balances multi-band capable clients by assigning bands to clients based on their capabilities. In the Band steering mode drop-down list optionally set the following Band Steering Mode options:
- *Band Steering to A band*: Infrastructure attempts to steer all A-Capable wireless clients to the 5 GHz band when they connect to this ESS.
 - *Band Steering to N band*: Infrastructure attempts to steer all N-Capable wireless client that are also A-Capable to the 5GHz band when they connect to this ESS. Infrastructure also attempts to steer non N-Capable wireless clients to the 2.4 GHz band.
 - Band Steering Disabled
- 24.** In the *Band Steering Timeout* text box, optionally provide the number between 1-65535. *Band Steering Timeout* is the number of seconds that assignment for a steered client is blocked on the forbidden band while it is unassociated.
- 25.** In the *Expedited Forward Override* drop-down list, optionally enable override (on). The *Expedited Forward Override* option is implemented to Override the DSCP value of Expedited Forwarding to Class Selector CS6 in the IP-Header of the Voice Packet sent by WLAN Phones. This feature is specific to AP300 and is disabled by Default.
- 26.** The SSID Broadcast Preference is specific to address the CISCO phone connectivity issues. It consists of three options as follows:
- *Disable*: Configuring the parameter to "Disable" enables the AP to advertise the beacons as usual following the concept of CSSID.
 - *Always*: Configuring the parameter to "Always" enables the AP to advertise the SSID on the beacons always. This must not be configured unless recommended.
 - *Till-Association*: This is the default configuration. Configuring the parameter to "Till-Association" enables the AP to advertise the SSID in the beacons till association stage of the client and disable the SSID broadcast in the later part of connectivity. This parameter is preferable to configure for the certain version of phones which will resolves the connectivity issues with the VPort ON. Once station associated, AP320 will stop broad-

casting SSID string. Here the users are allowed to configure SSID broadcast for VPort parameter from controller GUI per ESS basis in addition to AP CLI.

27. In the *Enable Countermeasure* list, select whether to enable or disable MIC Countermeasures:
- *On*: (The default) Countermeasures are helpful if an AP encounters two consecutive MIC errors from the same client within a 60 second period. The AP will disassociate all clients from the ESSID where the errors originated and does not allow any clients to connect for 60 seconds. This prevents an MIC attack.
 - *Off*: Countermeasures should only be turned off temporarily with this option while the network administrator identifies and then resolves the source of a MIC error.
28. Multicast MAC Transparency feature enables MAC transparency for tunneled multicast, which is needed for some clients to receive multicast packets. Multicasting is an advanced feature and can cause subtle changes in your network. By default, multicasting is disabled. Optionally enable *Multicast MAC*:
- *On*: All downstream multicast packets will have the MAC address of the streaming station.
 - *Off*: Default - all downstream multicast packets will have the MAC address of the controller.
29. In the *Supported and Base Transmit Rates* for each of the modes, enable or disable rates as needed.
30. In the *Voice Client Type*, select the type from the drop-down list. This field is configured when the set up comprises of Ascom or Spectralink phones.

See the **Configuring an ESS** chapter of the **Controller Configuration Guide**, for detailed information on *ESS Profiles*.

Security Profile in FortiWLM

As the networks of the world have united into a single, globe-spanning behemoth, security has taken on new importance. Wireless LANs were once the bane of security-conscious networking organizations, but newer tools make it easier to build networks with significant security protections. In addition to traditional security issues such as traffic separation between user groups and maintaining appropriate access privileges, wireless networks present new challenges, like rogue access points and unauthorized clients.

The Security profiles can be configured either from FortiWLM or from the controller. The security options is enforced by creating security profiles that are assigned to a service profile. As such, they can be tailored to the services and the structure (virtual LAN, Virtual Cell, etc.) offered by the ESSID and propagated to the associated APs. You can tell where a profile was configured by checking the read-only field *Owner* (*WLAN > Configuration > Wireless > ESS*); the *Owner* is either *nms-server* or *controller*. Each service profile must be associated with ESS and security profiles. To add a security from the *NM* web UI, follow these steps:

1. Navigate to *Configuration > Templates > Wireless Service*. The *Service Profile* screen displays a list of Service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit*. The following tabs are displayed:
 - Service Profile
 - Registration
 - ESS Profile
 - Security Profile
3. Select the *Security Profile* tab, the *Service Profile - Security Profile* screen provides a list of parameters that define how security is handled within a service profile. With security profiles, you can define the Layer 2 security method, including the cipher suite, static WEP key entries and key index position, and other parameters. The various security profiles you create allow you to support multiple authentication and encryption methods within the same NM infrastructure. [Figure 44 on page 114](#) illustrates the *Service Profile - Security Profile* screen.

Figure 44: Service Profile - Security Profile

Service Profile: Scale_ServicePro_911 ?

Service Profile Registration ESS Profile **Security Profile** VLAN Profile

Security Profile Name: Scale_SecurityPro_911

▼ SECURITY SETTINGS

Security Mode: Open ▼

▼ CAPTIVE PORTAL SETTINGS

Captive Portal: Disabled ▼

▼ MAC FILTERING SETTINGS

MAC Filtering: Off ▼

▼ FIREWALL SETTINGS

Firewall Capability: None ▼

▼ GENERAL SETTINGS

Security Logging: Off ▼

4. Individual *Security Profiles* can also be created by clicking *Configuration > Profiles > Security > Add*. The *Security Profile - Add* screen allows you to create a new security profile and complete the profile by providing data in all fields. This security profile will not be linked to any configuration yet, but will be available to one or all configurations that you

create in the future. The Security that you create this way will appear in the drop-down box labeled Security for all configurations.

5. In the *L2 Modes Allowed* area, select one of the following *Layer 2* security modes:
 - *Clear*: The WLAN does not require authentication or encryption, and the WLAN does not secure client traffic. This is the default setting.
 - *802.1x*: Can provide 802.1X authentication and WEP64 or WEP128 encryption.
 - *Static WEP keys*: Requires that stations use a WEP key.
 - *WPA*: Requires 802.1X Radius server authentication with one of the EAP types. Radius profiles are configured in the Service Profile.
 - *WPA-PSK*: Uses the TKIP encryption and requires a Pre-shared key.
 - *WPA2*: Requires 802.1x Radius server authentication with one of the EAP types. Radius profiles are configured in the Service Profile.
 - *WPA2-PSK*: Uses the CCMP-AES encryption and requires a Pre-shared key.
 - *MIXED*: Allows both WPA and WPA2 clients using a single security profile.
 - *MIXED PSK*: Allows pre-shared key clients to use a single security profile.
 - *WAI*: Security profile using WAPI certificate mode.
 - *WAI PSK*: Security profile using WAI with a pre-shared key. This key can be in either alphanumeric or hex format, and must be between 8 to 64 characters.



Security profiles with L2 Mode 802.1x/WPA/?WPA2/MIXED only requires Radius profile. The Radius profile specified in the service profile will be synced to the controller only if the security profile comprises of 802.1x/WPA/?WPA2/MIXED L2 Modes.

6. In the *Data Encrypt* area, select one of the following (available choices are determined by the L2 Mode selected in the previous step):
 - *WEP64*: A 64-bit WEP key is used to encrypt packets.
 - *WEP128*: A 128-bit WEP key is used to encrypt packets.
 - *TKIP*: Encryption algorithm used with
 - *CCMP-AES*: A 128-bit block key is used to encrypt packets with WPA2.
 - *CCMP/TKIP*: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol replaces both TKIP, the mandatory protocol in WPA, and WEP, the earlier, non-secure protocol.
 - *WPI-SMS4*: The encryption algorithm used for encrypting and decrypting messages in WAI-enabled profiles.

If you select *WEP64* or *WEP128*, you need to specify a WEP key in the next step. If you specify *TKIP* for *WPA-PSK* or *CCMP-AES* for *WPA2-PSK*, set a pre-shared key.
7. In the *WEP Key* text box, specify a WEP key. If you selected *Static WEP Keys* option, you need to specify a WEP key in hexadecimal or text string format. A WEP64 key must be 5 octets long, which you can specify as 10 hexadecimal digits (the hexadecimal string must

be preceded with 0x) or 5 printable alphanumeric characters (the ! character cannot be used). For example, 0x619B947A3D is a valid hexadecimal value, and wpass is a valid alphanumeric string. A WEP128 key must be 13 octets long, which you can specify as 26 hexadecimal digits (the hexadecimal string must be preceded with 0x) or 13 printable alphanumeric characters (the ! character cannot be used). For example, 0xB58CE2C2C75D73B298A36CDA6A is a valid hexadecimal value, and mypass8Word71 is a valid alphanumeric string.

8. In the *Static WEP Key Index* text box, type the index number to be used with the WEP key for encryption and decryption. A station can have up to four static WEP keys configured. The static WEP key index must be an integer between 1 through 4 (although internal mapping is performed to handle wireless clients that use 0 through 3 assignments).
9. In the *Re-Key Period* text box, type the duration that the key is valid. Specify a value from 0 to 65,535 seconds. The default re-key value is zero (0). Specifying 0 indicates that re-keying is disabled, which means that the key is valid for the entire session, regardless of the duration.
10. In the *BKSA Caching Period* text box, enter the desired period for which the BKSA value will be cached (in seconds). Note that this field is only used in WAPI configurations, and will otherwise be disabled. Specify a value from 0 to 65,535 seconds. The default caching period value is 43200.
11. In the *Captive Portal* drop-down list, select one of the following:
 - *Disabled*: Disables the Captive Portal.
 - *WebAuth*: Enables a WebAuth Captive Portal for users to log into. This feature can be set for all L2 Mode selections.
12. Captive portal profiles allows you to create individual captive portal profiles with distinct configuration settings. Such captive portal profiles can be mapped to security profiles for fine control over captive portal user access. A captive portal profile is created from the **Configuration > Profiles > Captive Portal** page.

NOTE: Captive Portal profile can be enabled only if at least one Captive Profile is created.

13. If you want to use a third-party Captive Portal solution from a company such as Bradford, Avenda, or CloudPath change the value for *Captive Portal Authentication Method* to *external*.
14. If 802.1x is to be used, in the *802.1X Network Initiation* drop-down list, select one of the following:
 - *On*: The controller initiates 802.1X authentication by sending an EAP-REQUEST packet to the client. By default, this feature is enabled.
 - *Off*: The client sends an EAP-START packet to the controller to initiate 802.1X authentication. If you select this option, the controller cannot initiate 802.1X authentication.
15. If the *Static WEP Key* mode to be used, in the *Shared Key Authentication* list, select one of the following:
 - *On*: Allows 802.1x shared key authentication.

- *Off*: Uses Open authentication. By default, this feature is off.
16. In the *Pre-shared Key* text box, enter the key that is to be used if the WPA-PSK or WPA2-PSK option was selected in step 2 above. The key can be from 8 to 63 ASCII characters or 64 hex characters (hex keys must use the prefix "0x" or the key will not work).
 17. In the *Group Keying Interval* text box, enter the time in seconds for the interval before a new group key is distributed.
 18. In the PMK Caching list, select one of the following:
 - On: PMK caching is allowed.
 - Off: PMK caching is not allowed.
 19. In the *Key Rotation* drop-down list, select whether to enable or disable this feature.
 20. Indicate the *Backend Auth Server timeout* from zero milliseconds to 65535 milliseconds (about 1 minute, 5 seconds)
 21. In the *Reauthentication* drop-down list, select one of the following:
 - *On*: Controller honors and enforces the "Session-timeout" Radius attribute that may be present in a Radius Access-Accept packet. Use this option if the Session-timeout attribute is used to require stations to re-authenticate to the network (802.1X) at a specified period. If "Session-timeout" is not used, there is no reason to enable re-authentication.
 - *Off*: Disables re-authentication for this security profile.
 22. In the *MAC Filtering* drop-down list, select one of the following:
 - *On*: Enables MAC Filtering for this security profile.
 - *Off*: Disables MAC Filtering for this security profile.

Enabling Per ESS MAC Filtering

- In the **Configuration** > (Templates) Wireless Service page, specify the Primary Authentication RADIUS and the Primary MAC AUTH RADIUS and click the Save button. This will create the RADIUS profile tabs
- In the RADIUS profile tab, configure Primary authentication and Mac Filtering Primary.
- In the Security profile, ensure that the MAC Filtering is ON.



Configure Primary authentication before configuring Mac Filtering Primary parameters.

23. In the ACL Environment State, select one of the following:
 - Disabled: The local ACL list is not used for MAC filtering.
 - Permit List Enabled: Only the MAC address in this list is allowed.
 - Deny List Enabled: Only the MAC address in this list is blocked.
24. In the *Firewall Capability* drop-down list, select one of the following:
 - *Configured*: The controller defines the policy through configuration of the Firewall Filter-ID.

- *Radius-configured*: The Radius server provides the policy after successful 802.1X authentication of the user. This option requires the Radius server have the filter-id configured. If this is not configured, the firewall capability is not guaranteed.
 - *None*: Disables the Firewall Capability for this security profile.
25. In the *Firewall Filter ID* text box, enter the firewall filter-id that is used for this security profile. The filter-id is an alphanumeric value that defines the firewall policy to be used on the controller, when the firewall capability is set to configured. For example, 1.
26. In the *Security Logging* drop-down list, select one of the following:
- On: Enables logging of security-related messages for this security profile.
 - Off: Disables logging of security-related messages for this security profile.
27. In the *Passthrough Firewall Filter ID* text box, enter a firewall filter ID. The filter ID is an alphanumeric value that defines the firewall policy to be used on the controller for a Captive Portal-enabled client that has no authentication.
28. *802.11W - Management Frame Protection*: Select **Capable** to enable management frame protection for 802.11w capable clients or select **Enable** to enable management frame protection for all clients.
29. *Tunnel Termination* allows you to perform configuration on per-security profile basis. Select one of the following in the *Tunnel Termination* drop-down list.
- *PEAP*: PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. It is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control. It authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS)
 - *TTLS*: TTLS (Tunneled Transport Layer Security) is a proposed wireless security protocol.



When Tunnel Termination is enabled, Fortinet's default certificate is used. In this case, the certificate must be "trusted" on the wireless client end in order for authentication to be successful. Refer to Security Certificates for details on how to import a certificate.

When PEAP/TTLS is configured on the RADIUS server, PEAP/TTLS termination should be disabled.

See the **Configuring Security** chapter of the **Controller Configuration Guide**, for detailed information on *Security Profiles*.

RADIUS Profile

RADIUS (Remote Authentication Dial-In User Service) enables you to use up to three servers (one primary server and one or two backups) and maintain separate authentication and accounting for each RADIUS server employed. For authentication, this allows a different password for each user instead of having to rely on maintaining and distributing switch-specific passwords to all users. For accounting, this can help you track network resource usage.

If you have a RADIUS accounting server in your network, you can configure the controller to act as a RADIUS client, allowing the controller to send accounting records to the RADIUS accounting server. The controller sends accounting records either for clients who enter the wireless network as 802.1X authorized users or for the clients that are Captive Portal authenticated.

When using RADIUS accounting, set up a separate RADIUS profile for the RADIUS accounting server and point the *Service Profile* to that RADIUS profile. So, for example, you could have a RADIUS profile called radiusprofile1 that uses UDP port 1645 or 1812 (the two standard ports for RADIUS authentication) and your service profiles would point to radiusprofile1. To support RADIUS accounting, configure a new RADIUS profile (like radiusprofile1_acct) even if the RADIUS accounting server is the same as the RADIUS authentication server. Set its IP and key appropriately and set its port to the correct RADIUS accounting port (1646, 1813 for example). Then point *Service Profiles* to this new RADIUS profile radiusprofile1_acct.

The *RADIUS Profiles* can be either be *common* to all controllers or *specific* to one controller. *Common RADIUS* profiles apply to all controllers registered to a service profile. A *controller-specific* RADIUS profile, is specific to one controller. If both the types of RADIUS profiles are on a controller, the controller-specific RADIUS profile takes precedence over a common RADIUS profile. If you want to use a common RADIUS profile instead of controller-specific, delete the controller-specific RADIUS profile.

Remote RADIUS Server

Network deployments with remote sites that are physically away from their head-quarter (or master data center -DC) can use remote RADIUS server in each of the remote sites for local authentication purposes.

In a typical scenario, a RADIUS server is usually co-located in the DC. Remote sites that required AAA services to authenticate their local clients use the RADIUS server in the DC. This in most cases introduces among other issues high latency between the remote site and its DC. Deploying a RADIUS server within a remote site alleviates this problem and allows remotes sites or branches to use their local AAA services (RADIUS) and not rely on the DC.

Before you Begin

Points to note before you begin deploying a remote RADIUS server:

1. Ensure that the Controller and the site AP communication time is less than RADIUS timeout.
2. Provision for at least one AP that can be configured as a relay AP.
3. Only Fortinet 11ac APs (AP122, AP822, AP832, and OAP832) in L3-mode can be configured as a relay AP.
4. In case of WAN survivability, no new 802.1x radius clients will be able to join, until relay AP rediscovers the controller.

5. Remote radius profile configurations are not supported in the common radius profile creation.

How It Works

This feature provides local authentication (.1x, Captive Profile, and mac-filtering) services using a RADIUS server set up in the remote site. In addition to the RADIUS server, the remote site must also configure a Fortinet 11ac AP as a relay AP. The remote RADIUS profile can be created using FortiWLM's WebUI (Configuration > Profiles > RADIUS). A remote RADIUS profile works like a regular profile and can be used as primary and secondary RADIUS auth and accounting servers.



High latency between the remote site and DC can cause client disconnections and sluggish network experience.

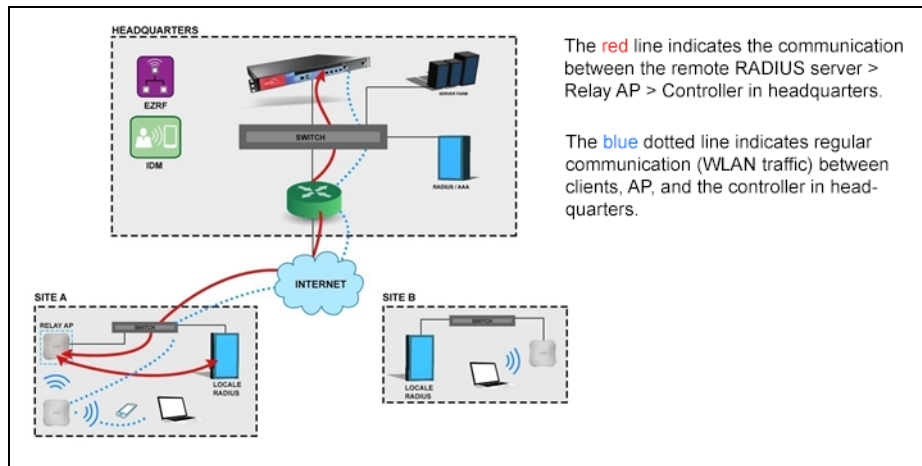
About Relay AP

The relay AP primarily is used for communicating between the RADIUS server (in the remote site) and the controller in the head-quarters.

An AP is set as a relay AP only when it is assigned in the RAIDUS profile. Once an AP is assigned as a relay AP It is recommended that you do not overload the relay AP with client WLAN services. This can result in communication issues between the relay AP and DC. For regular client WLAN services, we recommend the use of a different Fortinet access point.

For a remote RAIDUS profile, you cannot configure a secondary relay AP. However, for resilience purposes, we recommend configuring an alternate (backup) RADIUS profile and assigning another AP as a relay AP to this backup RAIDUS profile. In the security profile, set this RADIUS profile as the secondary RADIUS server.

The following figure illustrates a simple scenario with local RADIUS deployment



While creating the RADIUS profile in the FortiWLM (**Configuration > Profiles > RADIUS**), enable Remote RADIUS Server and select a Relay AP (see the screenshot).

RADIUS Profile - Add ?

RADIUS Profile Name *	<input type="text"/>	[1-16] chars.,
Description	<input type="text"/>	[0-128] chars.
RADIUS IP *	<input type="text"/>	
RADIUS Secret *	<input type="text"/>	[1-64] chars.
RADIUS Port *	<input type="text" value="1812"/>	Valid range: [1024-65535],
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	
Called-Station-ID Type	<input type="text" value="Default"/>	
COA	<input type="text" value="On"/>	
Controller Name	<input type="text" value="10.128.0.31"/>	
Remote Radius Server	<input type="text" value="Off"/>	
Remote Radius Relay AP ID	<input type="text"/>	
RADIUS Server Timeout	<input type="text" value="2"/>	Valid range: [1-20],
RADIUS Server Retries	<input type="text" value="3"/>	Valid range: [1-10],

To complete the *RADIUS Profile*, follow these steps:

1. *Common RADIUS profiles* are created by navigating to, *Configuration > Templates > Wireless Service > Choose a Service Profile > Select Edit option > Service Profile - Update screen*. If you don't see a *RADIUS Profile* tab, then the selected service profile does not have one configured. Provide the data for the following fields:
 - Primary Authentication
 - Secondary Authentication
 - Primary Accounting
 - Secondary Accounting
 - Primary MAC Auth RADIUS
 - Secondary MAC Auth RADIUS

The RADIUS created using the above method appears in the drop-down list is the labeled as RADIUS for all configurations. The above names can be up to 16 alphanumeric characters long with no spaces. This is an optional field.

2. Provide the information for the following fields in the *Primary Authentication* and *Secondary Authentication* tabs: (*Figure 45 on page 124* illustrates the *Service Profile - RADIUS Profile* screen.)
 - In the *Description* text box, provide some description about the RADIUS profile. A maximum of 128 characters of text can be added.
 - In the *RADIUS IP* text boxes, add the IP address of the RADIUS server.
 - In the *RADIUS Secret* text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.
 - In the *RADIUS Port* text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS accounting server, which uses port 1813 by default.
 - In the *MAC Address Delimiter* drop-down list, select the delimiter used on the RADIUS server to separate MAC addresses.
 - *None* - No delimiter is used.
 - *Hyphen (-)* - A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
 - *Single Hyphen (-)* - Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
 - *Colon (:)* - A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
 - In the *Password Type* drop-down list, select the type of password to be used for clients:
 - *Shared Key*--Uses the RADIUS secret that is configured.
 - *MAC Address*--Uses the client's MAC Address.

Figure 45: Service Profile - RADIUS Profile

RADIUS Profile - Add

RADIUS Profile Name *	<input type="text"/>	[1-16] chars.,
Description	<input type="text"/>	[0-128] chars.
RADIUS IP *	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
RADIUS Secret *	<input type="text"/>	[1-64] chars.
RADIUS Port *	<input type="text" value="1812"/>	Valid range: [1024-65535],
MAC Address Delimiter	Hyphen (-) ▼	
Password Type	Shared Key ▼	
Called-Station-ID Type	Default ▼	
COA	On ▼	
Controller Name	10.128.0.31 ▼	
Remote Radius Server	Off ▼	
Remote Radius Relay AP ID	▼	
RADIUS Server Timeout	<input type="text" value="2"/>	Valid range: [1-20],
RADIUS Server Retries	<input type="text" value="3"/>	Valid range: [1-10],

3. Accounting records are sent for the duration of a client session, which is identified by a unique session ID. You can configure a RADIUS profile for the primary accounting RADIUS server and another profile for a secondary accounting RADIUS server, which serves as a backup should the primary server be offline. The switch to the backup RADIUS server works as follows. After 30 seconds of unsuccessful Primary RADIUS server access, the secondary RADIUS server becomes the default. The actual attempt that made it switch is discarded and the next RADIUS access that occurs goes to the Secondary RADIUS server. After about fifteen minutes, access reverts to the Primary RADIUS Server. Provide the information for the following fields in the *Primary Accounting* and *Secondary Accounting* tabs:

- In the *Description* text box, provide some description about the RADIUS profile. A maximum of 128 characters of text can be added.
- In the *RADIUS IP* text boxes, add the IP address of the RADIUS server.
- In the *RADIUS Secret* text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.

- In the *RADIUS Port* text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS accounting server, which uses port 1813 by default.
 - In the *MAC Address Delimiter* drop-down list, select the delimiter used on the RADIUS server to separate MAC addresses.
 - *None* - No delimiter is used.
 - *Hyphen (-)* - A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
 - *Single Hyphen (-)* - Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
 - *Colon (:)* - A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
 - In the *Password Type* drop-down list, select the type of password to be used for clients:
 - *Shared Key*--Uses the RADIUS secret that is configured.
 - *MAC Address*--Uses the client's MAC Address.
4. *MAC Filtering options are specified in the MAC Filtering Primary and MAC Filtering Secondary tabs:*

The screenshot displays the 'RADIUS Profile' configuration window. The 'Mac Filtering Primary' tab is selected. The 'Common RADIUS Configuration' section includes the following fields:

- Description:** [Empty text box] [0-128] chars.
- RADIUS IP*:** [Four empty IP address boxes] Required
- RADIUS Secret*:** [Empty text box] [1-64] chars., Required
- RADIUS Port*:** [1812] Valid range: [1024-65535], Required
- MAC Address Delimiter:** [Hyphen (-) ▼]
- Password Type:** [Shared Key ▼]
- Called-Station-ID Type:** [Default ▼]
- COA:** [On ▼]

5. *Controller specific RADIUS profiles* are created by navigating to, *Configuration > Templates > Wireless Service > Choose a Service Profile > Select Edit option > Service Profile - Update screen > Choose the Radius Profile tab > Select Primary Authentication tab > Select the Add or plus icon* to add individual controller radius configuration.
6. *Configuration > Profiles > Radius > Radius Profile screen > Select the Add or plus icon* to add individual controller radius configuration. Controller specific RADIUS profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was

configured by checking the read-only from the controller, by selecting *Wireless > Configuration > Security > RADIUS* and look at the field *Owner*. A controller configuration owned by FortiWLM has the owner listed as *nms-server*.

7. Provide the information for the following fields in the *Radius Profile - Add* screen:

- In the *RADIUS Profile Name*, provide a name for the controller specific RADIUS profile. A maximum of 16 characters of text can be added.
- In the *Description* text box, provide some description about the RADIUS profile. A maximum of 128 characters of text can be added.
- In the *RADIUS IP* text boxes, add the IP address of the RADIUS server.
- In the *RADIUS Secret* text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.
- In the *RADIUS Port* text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS accounting server, which uses port 1813 by default.
- In the *MAC Address Delimiter* drop-down list, select the delimiter used on the RADIUS server to separate MAC addresses.
 - *None* - No delimiter is used.
 - *Hyphen (-)* - A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
 - *Single Hyphen (-)* - Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
 - *Colon (:)* - A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
- In the *Password Type* drop-down list, select the type of password to be used for clients:
 - *Shared Key*--Uses the RADIUS secret that is configured.
 - *MAC Address*--Uses the client's MAC Address.
- In the *Controller Name* drop-down list, select a controller IP address to which you want the RADIUS profile to be mapped.

See the **Authentication** chapter of the **Controller Configuration Guide**, for detailed information on *RADIUS Profiles*.

Hotspot 2.0 Profile in FortiWLM

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between WiFi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.

Adding a Hotspot 2.0 Profile

The Hotspot Profiles can be created from the **Configuration > Profiles > Hotspot 2.0** page. By default, the page shows the following details about a Hotspot profile.

Monitor

Configuration

RADIUS

Captive Portal

Captive Portal Exemptions

VLAN

Vlan Pool

Timer

GRE

Hotspot 2.0

Hotspot Profile (2)

REFRESH

ADD

EDIT

DELETE

VIEW

HOTSPOT PROFILE NAME	DESCRIPTION	INTERNET CONNECTIVITY	VENUE TYPE	ACCESS NETWORK TYPE	OPERATOR LANGUAGE CODE	OPERATOR LANGUAGE CODE	VENUE LANGUAGE CODE	VENUE LANGUAGE NAME	VENUE LANGUAGE CODE	VENUE LANGUAGE NAME	ASRA FLAG	LINK STATUS STATE	SYMMETRIC LINK	AT CAPACITY	OSAP ENABLED
meg-hs1		Unspecified	Unspecified	Private Network	English	English	English		English		Off	None	No	No	Off
VENUE		Unspecified	Unspecified	Private Network	English	English	English		English		Off	None	No	No	Off

- **Hotspot Profile Name** - Displays the name of the Hotspot Profile.
- **Description** - Displays the Description provided for the Hotspot profile.
- **Venue Type** - Displays the Venue Type.
- **Access Network Type** - Select the Access Network Type from the list. The default selection is displayed as Private Network. The types are as follows:
 - Private Network
 - Private Network with Guest Access
 - Chargeable Public Network
 - Free Public Network
 - Personal Device Network
 - Emergency Services Only Network
 - Test or Experimental Network
 - Wildcard Network
- **IPv6 Availability** - Select the IPv6 Availability from the list. The default selection is displayed as Address type not available. The types are as follows:
 - Address type available
 - Address type not available
 - Availability of the Address type not known
- **IPv4 Availability** - Select the IPv4 Availability from the list. The default selection is displayed as Address type not available. The types are as follows:
 - Address type available

- Address type not available
- Availability of the Address type not known
- Port-restricted IPv4 address available
- Single NATed private IPv4 address available
- Double NATed private IPv4 address available
- Port-restricted IPv4 address and single NATed IPv4 address available
- Port-restricted IPv4 address and double NATed IPv4 address available
- **Roaming Consortium** - Enter the roaming ORG ID for the Hotspot profile. The valid range is 0-10 characters.
- **Operators** - Enter multiple network operators. Select a language and enter a name. The valid range is 0 - 256 characters.
- **Venue** - Enter multiple hotspot venues. Select a language and enter a name. The valid range is 0 - 256 characters.
- **3GPP Cell Network** - Provide the following details:
 - Country code of the operator.
 - Provide the 3GPP Cell Network MCC. The default value is displayed is 0. The Valid range is [0-999].
 - Provide the 3GPP Cell Network MNC. The default value is displayed is 0. The Valid range is [0-999].
- **Domain Name** - Provide the Domain Name. The valid range is [0-128] chars.
- **NAI Realm from 1-10** - Provide the NAI Realm [1-10] from the list. The valid range is [0-50] chars.
- **NAI Realm Auth Method from 1-10** - Select the NAI Realm Auth Method [1-10] from the list. The valid range is [0-50] chars. The types are as follows:
 - EAP TLS Certificate
 - EAP TTLS MSCHAPv2 Username/Password
 - EAP SIM
 - EAP AKA
 - EAP AKA'
- **Advanced Settings** - Provide the following configuration details for advanced settings:
 - HESSID - An AP's Homogenous ESS Identifier (HESSID), which is that device's MAC address in colon-separated hexadecimal format.
 - GTK Per Station - Enables the Group Temporal Key (GTK) to be assigned per station.
 - Gas Come Back Flag - Enables the Generic Advertisement Service (GAS) comeback request/response option.

- Gas Come back Delay (milliseconds) - At the end of the GAS comeback delay interval, the client can attempt to retrieve the query response using the comeback request action frame.
- ASRA Flag - Enable the Additional Step Required for Access (ASRA) to indicate that the network requires one more step for access.
- Authentication type - Configure the network authentication type required as per ASRA. Supported values are, Acceptance of terms and conditions, On line enrolment supported, http/https redirection, and DNS redirection.
- Redirect URL - Specify the Redirect URL in case of http/https redirection and DNS Redirection.
- **WAN Metrics** - Provide the following configuration details for WAN metrics:
 - Link Status State - Select the status of the WAN link.
 - Symmetric Link - Enable symmetric bandwidth.
 - At Capacity - Select whether the WAN link is at capacity and no additional mobile devices will be allowed to associate with the AP.
 - Down Link speed/Up Link speed - The WAN Backhaul link for current downlink/uplink speed in KBPS.
 - Down Link load/Up Link load - The current percentage load of the downlink/uplink connection, measured over an interval the duration of which is reported by the Load Measurement Duration.
 - Load Measurement Duration - The duration over which the downlink/uplink load is measured in KBPS.
 - Connection CapabilityThe Connection Capability enables filtering of protocols, allowing or restricting traffic on some protocols and ports. A set of system defined protocols as listed. Additionally, you can also create rules for custom protocols.
- **QoS Map** - Create a Quality of Service (QoS) policy by configuring the following DSCP ranges and DSCP exceptions.
 - DSCP Ranges - For a given DSCP range, specify the User Priority (valid range: 0 -7), DSCP High Priority (valid range: 0 - 255), and DSCP Low Priority (valid range: 0-255).
 - DSCP Exceptions - For a given DSCP exception, specify the User Priority (valid range: 0 -7) and the DSCP Value (valid range: 0 - 255).
- **OSU Settings** - The Online Sign Up (OSU) Service settings configures one or more Hotspot providers offering OSU service.
 - Online Sign Up Support - Select to enable OSU.
 - OSEN Enable - Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type. This network provisions clients using the OSU functionality.
 - OSU/OSEN ESSID - Specify the OSU ESSID.
 - OSU Server URL - Specify the URL of the OSU server.

- OSU NAI - Specify the OSU NAI for authentication.

Click Settings to configure the OSU provider settings.

- OSU Provider Friendly Names
- OSU Provider Icons
- OSU Provider Method - Select one of the OSU provider provisioning methods, OMA-DM or SOAP-XML.
- OSU Provider Description - The description of the OSU Provider.

Select **OK**. The Hotspot Profile is added and displayed on the Hotspot Profile screen.

The following operations can be performed on the Hotspot 2.0 profile.

- **Delete** - Select a Hotspot Profile and click **Delete**. The selected Hotspot Profile gets deleted from the Hotspot Profile screen.
- **Edit** - Select a Hotspot Profile and click **Edit**.
- **View** - Allows to view the details of the Hotspot Profile. Select a Hotspot Profile and click **View**.

VLAN Profile in FortiWLM

A virtual local area network (VLAN) is a broadcast domain that can span across wired or wireless LAN segments. Each VLAN is a separate logical network. Several VLANs can coexist within any given network, logically segmenting traffic by organization or function. In this way, all systems used by a given organization can be interconnected independent of physical location. This has the benefit of limiting the broadcast domain and increasing security. VLANs can be configured in software, which enhances their flexibility. VLANs operate at the data link layer (OSI Layer 2), however, they are often configured to map directly to an IP network, or subnet, at the network layer (OSI Layer 3). You can create up to 512 VLANs.

IEEE 802.1Q is the predominant protocol used to tag traffic with VLAN identifiers. VLAN1 is called the default or native VLAN. It cannot be deleted, and all traffic on it is untagged. A trunk port is a network connection that aggregates multiple VLANs or tags, and is typically used between two switches or between a switch and a router. VLAN membership can be port-based, MAC-based, protocol-based, or authentication-based when used in conjunction with the 802.1x protocol. Used in conjunction with multiple ESSIDs, VLANs support multiple wireless networks on a single Access Point using either a one-to-one mapping of ESSID to VLAN, or mapping multiple ESSIDs to one VLAN. By assigning a security profile to a VLAN, the security requirements can be fine-tuned based on the use of the VLAN, providing wire-like security or better on a wireless network.

VLANs can be configured/owned either by *FortiWLM* or by a controller. You can tell where a profile was configured by checking the read-only field *Owner*; the *Owner* is either *nms-server*

or *controller*. All *nms-server* VLAN profiles cannot be modified on the controller. In order to map a service profile to a VLAN, follow the below steps:

1. Select *Configuration > Templates > Wireless Service > Choose a Service Profile > Select Edit option > Service Profile - Update* screen.
2. In the *Service Profile - Update* screen, Select the *Tunnel Interface Type* from the drop-down list. The following are the options:
 - *No Tunnel*: No tunnel is associated with this service profile.
 - *Configured VLAN Only*: A configured VLAN only is listed in the following VLAN Name list is associated with this service profile.
 - *Radius VLAN Only*: The VLAN is assigned by the RADIUS server via the RADIUS attribute Tunnel Id. Use RADIUS VLAN Only when clients authenticate via 802.1x/WPA/WPA2 or MAC Filtering.
 - *Radius and Configured VLAN*: Both configured VLAN and RADIUS VLAN are associated with this service profile.
 - *GRE*: Specifies a GRE Tunnel configuration.

This is an optional field.

3. If you have selected the *Tunnel Interface Type* as *Configured VLAN Only*, *Radius VLAN Only*, and *Radius and Configured VLAN*, type a *VLAN Profile* name or select an existing *VLAN Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
Configuration > Templates > Wireless Service > Service Profile > Edit > Service Profile - Update > provide a name in the *VLAN Profile* text box or select the existing *VLAN Profile*. The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
4. Select the *VLAN Profile* tab, click the *Add or plus* icon to add individual controller VLAN configuration. The controller specific VLAN profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Wireless > Configuration > Security > VLAN* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
5. To add individual VLAN profiles, select *Configuration > Profiles > VLAN > Add*. Provide the information for the following fields in the *VLAN Profile - Add* screen:
 - Provide a *VLAN Profile Name* up to 32 alphanumeric characters long without spaces for the VLAN Profile Name. This is a required field.
 - In the *TAG* text box, either type the VLAN tag or select the VLAN tag. The VLAN tag is an integer in the range of 1 through 4,094. This is a mandatory field.
 - In the *Fast Ethernet Interface Index* text box, enter the number of the interface (1 or 2; the second interface is an optional configuration).
 - In the *IP Address* text boxes, type the IP address. The IP address must match the IP address of the default gateway configured in wireless clients.

- In the *Netmask* text boxes, type the subnet mask of the IP address. The subnet mask must match the subnet mask of the default gateway configured in wireless clients.
 - In the *IP Address of the Default Gateway* text boxes, type the default gateway's IP address. This IP address is the default gateway used by the controller to route traffic from clients using this VLAN.
 - In the *Override Default DHCP Server Flag* drop-down list, select one of the following options:
 - *On*: Enable use of specified DHCP server (see step 8 rather than the global DHCP server configured for the controller).
 - *Off*: Disable usage of specified DHCP server and return to using global DHCP server configured for the controller.
 - In the *DHCP Server IP Address* text boxes, type the IP address of the DHCP relay server.
 - In the *DHCP Relay Pass-Through* drop-down list, select one of the following options:
 - *On*: Enable use of the pass-through DHCP server feature (default setting).
 - *Off*: Disable usage of the pass-through DHCP server feature. If the DHCP server is set to the default IP address of 127.0.0.1, DHCP packets pass through without modification. No DHCP relay function is performed. Instead, the packet is copied as is. This mode of operation is the default for a fresh system.
 - In the Controller Name drop-down list, select a controller IP address.
6. Select **Save**. The VLAN Profile is created and displayed on the VLAN Profile screen. [Figure 46 on page 133](#) illustrates the *Service Profile - VLAN Profile Add* screen.

Figure 46: Service Profile - VLAN Profile - Add

VLAN Profile - Add ?

VLAN Profile Name *	<input type="text"/>	[1-32] chars.,
TAG *	<input type="text"/>	Valid range: [1-4094],
Ethernet Interface Index *	<input type="text"/>	Valid range: [1-2],
IP Address *	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Netmask *	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Default Gateway *	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Override Default DHCP Server Flag	<input type="text" value="Off"/>	
DHCP Server IP Address *	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
DHCP Relay Pass-Through	<input type="text" value="On"/>	
Controller Name	<input type="text"/>	
Maximum number of clients	<input type="text"/>	Integer



VLAN profiles cannot be edited once they are synchronized to a controller.

Modify the Existing VLAN Profile

All *VLAN Profiles* are edited differently, depending on whether or not they are synced to a controller. To edit a unsynced *VLAN Profile*,

1. Navigate to *Configuration > Templates > Wireless Service*. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit*.
3. Select the *VLAN Profile* tab, the *Service Profile - VLAN Profile Add* screen is displayed. [Figure 46 on page 133](#) illustrates the *Service Profile - VLAN Profile Add* screen.
4. Perform the modifications on the *Service Profile - VLAN Profile* screen and select *Save*. Updating a synced *VLAN Profile* is more complicated and can be done with two methods, as described below.

Edit a Synced VLAN by un-registering Controllers

To edit a VLAN synced to controllers, follow these steps:

1. Navigate to *Configuration > Templates > Wireless Service*. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit*. Un-register the controller(s) from all service profiles where this *VLAN Profile* is used
3. Choose a service profile where VLAN is used and select a *Registration* tab.
4. Select the existing profile and click Unregister.
5. Change the *VLAN Profile* by clicking *Configuration > Profiles > VLAN*, selecting a *VLAN Profile > Edit > making the changes > Save*.
6. Re-register the controller to all service profiles where this *VLAN Profile* is used by clicking *Configuration > Templates > Wireless Service > select a service profile where this VLAN is used > Registration tab > select the controller > Save*.

Edit a Synced VLAN by Editing Service Profiles

To edit a VLAN synced to controllers, follow these steps:

1. Edit all the service profiles where this VLAN is used by clicking *Configuration > Templates > Wireless Service > selecting a profile where VLAN is used > Edit > changing Tunnel Interface Type to No Tunnel > OK*.
2. Change the *VLAN Profile* by clicking *Configuration > Profiles > VLAN*, selecting a *VLAN Profile > Edit > making the changes > Save*.
3. Re-edit all the service profiles you changed in step 1 by clicking *Configuration > Templates > Wireless Service > selecting a profile > Edit > changing Tunnel Interface Type to the earlier value (Configured VLAN only or RADIUS VLAN only or Configured VLAN or GRE) > Save*.

See the **Configuring VLANs** chapter of the **Controller Configuration Guide**, for detailed information on *RADIUS Profiles*.

Rogue AP Detection

You can create a whitelist of APs that will perform rogue detection. Other APs that are not added to this whitelist will not scan for rogue AP/clients.

The rogue detection feature is available only if the global option for rogue detection is enabled.

If you have upgraded from an older (pre 8.1 build), all APs in the network are added to the Allowed APs list. You must manually remove from the AP list and keep or add AP required for rogue AP detection.

To configure an AP for rogue detection,

Go to Configuration > Rogue APs.

Create a profile and ensure that Detection is set to ON.

The screenshot shows a web-based configuration interface with three tabs: 'Allowed APs', 'Blocked APs', and 'Registered Controllers'. The 'Registered Controllers' tab is active. A modal dialog titled 'Add Rogue APs Profile' is open, featuring a close button (X) in the top right corner. The dialog contains the following fields and options:

- Rogue APs Profile**: A text input field containing 'rogue_ap'.
- Detection**: A dropdown menu set to 'On'.
- Mitigation**: A dropdown menu set to 'No mitigation'.
- Rogue AP Aging (seconds)**: A text input field with '600' and a 'Valid range: [60-86400]' note.
- Number of Mitigating APs**: A text input field with '3' and a 'Valid range: [1-20]' note.
- Scanning time in ms**: A text input field with '100' and a 'Valid range: [100-500]' note.
- Operational time in ms**: A text input field with '400' and a 'Valid range: [100-5000]' note.
- Max mitigation frames sent per channel**: A text input field with '10' and a 'Valid range: [1-50]' note.
- Scanning Channels**: A text input field with '1,2,3,4,5,6,7,8,9,10,11,12,13,' and a 'Enter 0-256 chars.' note.
- RSSI Threshold for Mitigation**: A text input field with '-100' and a 'Valid range: [-100-0]' note.

At the bottom right of the dialog are two red buttons: 'CANCEL' and 'SAVE'.

Click the push profile icon to push this profile. There are two ways to push the profile. When you select controllers running SD 8.0 or older version, the rogue detection profile is pushed to all APs.

Apply Rogue AP profile

Rogue APs Profile

rogue_ap

Scanning Options

☒ All APs on Controller ☐ Select APs

Controller

172.19.7.158

172.19.8.200

172.19.8.55

172.19.46.141

172.19.8.39

172.19.46.142

172.19.13.13

172.19.118.2

To select specific APs in the network, click Select APs to view APs running 8.1 release.

Apply Rogue AP profile

Rogue APs Profile

rogue_ap

1

2

Scanning Options

☐ All APs on Controller ☒ Select APs

Controller

x 172.18.201.205

	AP Name	Controller
<input checked="" type="checkbox"/>	AP-116	172.18.201.205
<input checked="" type="checkbox"/>	AP-117	172.18.201.205
<input type="checkbox"/>	AP-118	172.18.201.205
<input type="checkbox"/>	AP-111	172.18.201.205

CANCEL

SAVE

FORCE SYNC

VLAN POOL

To reduce big broadcast or risking a chance of running out of address space, you can now enable VLAN pooling in a wireless service profile.

VLAN pooling essentially allows administrators to create a named alias using a subset of VLANs thereby creating a pool of address. By enabling VLAN pool, you can now associate a client/device to a specific VLAN. This allows you to effectively manage your network by monitoring appropriate or specific VLANs pools.



VLAN Pool is available only in tunnelled mode.

Features

- You can associate up to 16 VLANs to a pool

- You can specify the maximum number of clients that can be associated to a VLAN.
- The client/device behavior does not change after it is associated to a VLAN in a pool.
- If a VLAN is removed from a VLAN pool, clients/devices connected to the VLAN will continue to be associated to the VLAN. However, if the clients disconnect and reconnect, their VLAN will change.

Creating a VLAN Pool

1. In the **Configuration** > (Profiles) **VLAN** page, create a VLAN.
2. Go to **Configuration** > (Profiles) **VLAN Pool** page, create a VLAN pool and specify the VLAN tag as mentioned in step 1.
3. In the **Configuration** > (Templates) **Wireless** page:
 - Select **Tunnel Type Interface** as VLAN Pool
 - Select the VLAN Pool Profile.

Time Based ESS Profile

You can schedule the availability of an ESS based on pre-define time intervals. By default, ESS profiles are always ON and available to clients/devices. By adding a timer, you can control the availability of an ESS profile based on pre-defined times during a day or across multiple days.

To create a time based ESS profile, you must first create a timer profile and then associate the timer profile to the ESS profile.

Creating a Timer Profile

You can create timer profile using WebUI or CLI.

Using WebUI

1. Go to **Configuration** > (Profiles) **Timer** and click the + button.
2. In the Add Timer Profile window, enter Timer Profile Name and select Timer Type:

TIMER Profile - Add

TIMER Profile Name

[1-32] chars., Required

Timer Profile Type

absolute

Service Start Time 1

Service End Time 1

Service Start Time 2

Service End Time 2

Service Start Time 3

Service End Time 3

- **Absolute** timer profiles can enable and disable ESS visibility for time durations across multiple days. You can create up to 3 specific start and end time per timer profile. To enter start of the end time, click the Date picker box. See label 1 in figure 1.
- **Periodic** timer profiles are a set of start and end timestamp that can be applied across multiple days of a week. To create a period timer profile, enter the time in hh:mm format. Where hh, represent hours in 2-digits and mm represent minutes in 2-digits. Figure 2, illustrates a timer profile that will be applied on Sunday, Monday, Tuesday, and Thursday from 08:10 a.m. or 14:45 (2.45 p.m)

TIMER Profile - Add

TIMER Profile Name

[1-32] chars., Required

Timer Profile Type

periodic

Days Of The Week

☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday

Time Interval Start 1

HH:MM

Time Interval End 1

HH:MM

Time Interval Start 2

HH:MM

Time Interval End 2

HH:MM

Time Interval Start 3

HH:MM

Time Interval End 3

HH:MM



Alternatively, while creating a wireless service, specify a name for the Timer profile before you click the Save button. After you click the Save button, additional tabs are opened to configure the timer-profiles.

GRE Profile in FortiWLM

The GRE tunneling provides packet isolation from one endpoint to another, encapsulated within an IP tunnel to separate user traffic. GRE tunneling provides an option to segregate users' traffic by allowing a service profile to be tied to a GRE profile. This provides an alternative to VLANs for segregating traffic.

GRE tunneling is accomplished by creating routable tunnel endpoints that operate on top of existing physical and/or other logical endpoints. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint. By design, GRE tunnels connect A to B and provide a clear data path between them. This data path is not secure. To ensure the data security, GRE uses *Internet Protocol Security* on the tunnels. These tunnels data is routed by the system to the GRE endpoint using routes established in the route table; therefore each data packet traveling over the GRE tunnel gets routed through the system twice.



The routes can be manually established or dynamically learned using routing protocols such as RIP or OSPF. Once a data packet is received by the GRE endpoint, it is encapsulated in a GRE header and routed again using the endpoint configuration destination address of the tunnel.

GRE can be configured/owned either by *FortiWLM* or by a controller. You can tell where a profile was configured by checking the read-only field *Owner*; the *Owner* is either *nms-server* or *controller*. All *nms-server* GRE profiles cannot be modified on the controller. In order to map a service profile to a GRE, follow the below steps:

1. Select *Configuration > Templates > Wireless Service > Choose a Service Profile > Select Edit option > Service Profile - Update* screen.
2. In the *Service Profile - Update* screen, Select the *Tunnel Interface Type* from the drop-down list. The following are the options:
 - *No Tunnel*: No tunnel is associated with this service profile.
 - *Configured VLAN Only*: A configured VLAN only is listed in the following VLAN Name list is associated with this service profile.
 - *Radius VLAN Only*: The VLAN is assigned by the RADIUS server via the RADIUS attribute Tunnel Id. Use RADIUS VLAN Only when clients authenticate via 802.1x/WPA/WPA2 or MAC Filtering.
 - *Radius and Configured VLAN*: Both configured VLAN and RADIUS VLAN are associated with this service profile.
 - *GRE*: Specifies a GRE Tunnel configuration.

This is an optional field.

3. If you have selected the *Tunnel Interface Type* as *GRE*, type a *GRE Profile* name or select an existing *GRE Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:

Configuration > Templates > Wireless Service > Service Profile > Edit > Service Profile - Update > provide a name in the *GRE Profile* text box or select the existing *GRE Profile*. The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.

4. Select the *GRE Profile* tab, click the *Add or plus* icon to add individual controller GRE configuration. The controller specific GRE profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Wireless > Configuration > Security > VLAN* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
5. To add individual GRE profiles, select *Configuration > Profiles > VLAN > Add*. Provide the information for the following fields in the *VLAN Profile - Add* screen:
 - In the
 - In the *Remote External Address* text boxes, type the IP address of the remote end of the GRE tunnel.
 - In the *Tunnel IP Address* text boxes, type the IP address for the local end of the GRE tunnel.
 - In the *Tunnel IP Netmask* text boxes, type the IP address.
 - In the *Local External FastEthernet Index* text box, type the interface ID (1 or 2; interface 2 requires configuration) of the *FastEthernet* interface that the tunnel will use.
 - In the *Override Default DHCP Server Flag* drop-down list, select the following options:
 - *On*: Enable use of specified DHCP server rather than the global DHCP server configured for the controller.
 - *Off*: Disable usage of specified DHCP server and return to using global DHCP server configured for the controller.
 - In the *DHCP Server IP Address* text boxes, type the IP address of the DHCP relay server.
 - In the *Controller Name* drop-down list, select a controller IP address.
6. Select *Save*. The *GRE Profile* is created and displayed on the *GRE Profile* screen.

Figure 47 on page 142 illustrates the *Service Profile - GRE Profile Add* screen



GRE profiles cannot be edited once they are synchronized to a controller.

Figure 47: Service Profile - GRE Profile - Add

Service Profile: test **GRE Profile - Add**

GRE Name	GRE_test			
Remote External Address	172	119	44	129
Tunnel IP address	255	255	255	0
Tunnel IP Netmask	172	19	44	111
Local External Ethernet Index*	1			Valid range: [1-2], Required
Override Default DHCP Server Flag	On ▾			
DHCP Server IP Address*				Required
Controller Name	172.19.43.227 ▾			

See the **Service Profile - GRE Profile** screen (*Configuration > Templates > Wireless Service > Edit > GRE Profile*) or the **GRE Profile - Add** screen (*Configuration > Profiles > Security > Add > GRE Profile - Add*) in Online Help for detailed information on *Security Profile* topic.

Modify the Existing GRE Profile

GRE profiles are edited differently, depending on whether or not they are synced to a controller. To edit an unsynced GRE profile,

1. Navigate to *Configuration > Templates > Wireless Service*. The *Service Profile* screen is displayed, providing a list of service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit*.
3. Select the *GRE Profile* tab.
4. In the *Service Profile - GRE Profile* screen, select a GRE Profile and click *Edit*. Perform the modifications and select *Save*. [Figure 47 on page 142](#) illustrates the *Service Profile - GRE Profile Add* screen.

Updating a synced GRE profile is more complicated and can be done with two methods, as described below.

Edit a Synced GRE Profile by un-registering Controllers

To edit a GRE synced to controllers, follow these steps:

1. Un-register the controller(s) from all service profiles where this GRE profile is used by clicking *Configuration > Templates > Wireless Service > select a service profile where GRE is used > Registration tab > select the controller > Unregister*.
2. Change the GRE profile by clicking *Configuration > Profiles > GRE*, selecting a GRE profile > *Edit > perform the changes > Save*.

3. Re-register the controller to all service profiles where this GRE profile is used by clicking Configuration > Templates > Wireless Service > select a service profile where GRE is used > Registration tab > Register > select the controller > Save.

Edit a Synced GRE Profile by Editing Service Profiles

To edit a GRE synced to controllers, follow these steps:

1. Edit all the service profiles where this GRE is used by clicking Configuration > Template > Wireless Service > selecting a profile where GRE is used > Edit > changing Tunnel Interface Type to No Tunnel > Save.
2. Change the GRE profile by clicking Configuration > Profiles > GRE, selecting a GRE profile > Edit > making the changes > Save.
3. Re-edit all the service profiles you changed in step 1 by clicking Configuration > Templates > Wireless Service > selecting a profile > Edit > changing Tunnel Interface Type to the earlier value (Configured VLAN only or RADIUS VLAN only or Configured VLAN or GRE) > Save.

See the **Configure GRE Tunnels** in the **Configuring Security** chapter of the **Controller Configuration Guide**, for detailed information on *GRE Profiles*.

Ethernet Profiles

An Ethernet Profile allows you to configure LACP settings which can be applied via an AP template.

Figure 48: Add New Ethernet Profile

AP Template - Add

Name	<input type="text" value="LACP ENABLE"/>	[1-32] chars., Required
Description	<input type="text" value="ENABLES LACP"/>	[0-128] chars.
Radio 1 Profile	<input type="text" value="Radio_1_bgn_profile"/>	▼
Radio 2 Profile	<input type="text" value="Radio_2_ac_profile"/>	▼
Radio 3 Profile	<input type="text" value="Radio_3_an_profile"/>	▼
Connectivity Profile	<input type="text" value="L2NOIP"/>	▼
Ethernet Profile	<input type="text" value="Enable_lacp"/>	▼
Auto-Sync	<input type="text" value="On"/>	▼

To create an Ethernet profile:

1. Go to **Configuration > Profiles > Ethernet** and click the '+' icon on the page.
2. In the **Ethernet Profile - Add** page, enter a name to identify the profile and select option to enable LACP.
3. Select the AP MAC assignment from the drop-down list.
4. Click **SAVE**.

Figure 49: *Add Ethernet Profile*

Ethernet Profile - Add

Ethernet Profile Name	<input type="text" value="Add LACP"/>	[1-32] chars., Required
LACP	<input type="button" value="Enable"/>	
AP MAC Assignment	<input type="button" value="eth0"/>	

To apply an Ethernet profile to an AP, the profile must be added to an AP template.

1. Go to **Configuration > AP Template** and select an AP template.
2. In the **AP Template: <template-name> - Update** page, select the Ethernet Profile from the drop-down list and click **SAVE**.

Captive Portal Profiles

The captive portal profiles feature that allows you to create individual captive portal profiles with distinct configuration settings. Such captive portal profiles can be mapped to security profiles for fine control over captive portal user access.

A captive portal profile is created from the **Configuration > Profiles > Captive Portal** page. Profile created in this page can be applied to a security profile.

NOTE: Captive Portal profile can be enabled only if at least one Captive Profile is created.

Social Authentication Support in Captive Portal

The captive portal authentication process now supports Fortinet Presence as an external CP authentication server that allows users to authentication using social media accounts like Facebook or Gmail OAuth.

Supported APs: AP122, AP822, AP832, OAP832, FAP-U421, and FAP-U423.

Before proceeding, note the following:

- Enable location service in the controller (See Configuring FortiPresence API section in the FortiWLC (SD) configuration guide for more details).
- Assign the AP in the data analytics store.

- Not supported in "Bridge mode"

To enable social authentication support, do the following:

Create Captive Portal Exemptions Profile

To enable social login, create a profile with the list of exempted URLs and in the captive portal profile and select FortiPresence as the external authentication server.

1. Go to Configuration > Profiles > Captive Portal Exemptions.

PROFILE NAME	DESCR	FQDN	ACTION
CP_Exemption1		c.com socialwifi.fortipresence.com	[Edit] [Delete]

1 - 1 of 1

2. Click the Add (+) button to create a profile with the list of URLs that will be allowed for social authentications. To add multiple URL to a profile, enter a space after each URL entry. You can add up to 32 URLs.

Edit Profile

Name: CP_Exemption1

Description:

FQDNs: c.com socialwifi.fortipresence.com

[SAVE] [CANCEL]



For each profile, ensure that you add **socialwifi.fortipresence.com** (inclusive of the 32 URLs) as part of the FQDN list. This is mandatory for clients to access Social Wi-Fi login page.

Configure Captive Portal Profile to use Fortinet Presence

1. Go to Configuration > Profiles > Captive Portal

2. Create a captive portal profile with local or radius as authentication type
 - If Authentication type is Local, then create a guest user with the following credentials (in the controller):
 - username: gooduser
 - password:good.
 - If Authentication type is RADIUS, then in that RADIUS server, create a user with the following credentials:
 - username: gooduser
 - password:good.

Make the following changes to External Portal Settings:

Captive Portal Configuration - Update ?

Captive Portal Name	CP_Exemption1		
Description	<input type="text" value=""/> [0-128] chars.		
Authentication Type	local ▼		
Primary Authentication RADIUS	<input type="text" value=""/> ▼		
Secondary Authentication RADIUS	<input type="text" value=""/> ▼		
Primary Accounting RADIUS	<input type="text" value=""/> ▼		
Secondary Accounting RADIUS	<input type="text" value=""/> ▼		
Accounting Interim Interval (seconds)	0 Valid range: [600-36000]		
External Port URL	<input type="text" value="http://socialwifi.fortipresence.com/wifi.htm"/> 1 [0-256] chars.		
Public IP of Controller	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Session Timeout(sec)	0 Valid range: [0-1440]		
Activity Timeout(sec)	0 Valid range: [0-60]		
Session caching Timeout(sec)	1 Valid range: [1-1440]		
Apple CNA Bypass	Off ▼		
Captive Portal External Server Type	Fortinet-Presence ▼ 2		
Captive Portal Exemption	CP_Exemption1 ▼ 3		

1. 1.Enter the <http://socialwifi.fortipresence.com/wifi.html?login> URL (1) in the external portal URL.
2. Select Fortinet-Presence as the external server (2).
3. Select the profile (3) created with the exempted URLs.

Enable this captive portal profile in security and ESS profiles

Enable the captive portal profile in the security profile and map the security profile in the ESS Profile. In the security profile, make the following changes to the CAPTIVE PORTAL SETTINGS section:

Security Profile - Add ⓘ

Security Profile Name*

FBAuthSecurity

[1 - 32] chars.,

▼ SECURITY SETTINGS

Security Mode

802.1x/Open

▼

802.1X Network Initiation

On

▼

Backend Auth Server Timeout

30

Valid range: [1-65535]

Reauthentication

On

▼

Tunnel Termination

☐ PEAP ☐ TTLS

▼ CAPTIVE PORTAL SETTINGS

Captive Portal

WebAuth

▼

Captive Portal Profile

FBAuth

▼

Captive Portal Authentication Method

external

▼

Passthrough Firewall Filter ID

[0-16] chars.

Templates

The *FortiWLM* provides the mechanism to set radio properties and connectivity properties for a set of APs. These radio and connectivity properties are applied to a group of APs from the *NM* server. The user groups having configuration permissions can only create, modify, and delete templates.

AP Template

An AP Template comprises of a *Connectivity Profile* and *Radio Profiles* applied to *Device Administration group* which is one of the classified form of AP Group. A *Connectivity Profile* comprises of the AP configuration parameters related to Network Connectivity. A Radio profile comprises of the configuration parameters which is applied on the wireless interface of the AP. Profiles can be created and applied to a set/group of APs from the *NM* server. Each Radio Profile can be configured individually via the controller or NM.

Figure 50 on page 148 illustrates the *AP Template* screen.

Figure 50: AP Template

AP Template

AP Template (3)							
NAME	DESCRIPTION	RADIO 1 PROFILE	RADIO 2 PROFILE	RADIO 3 PROFILE	CONNECTIVITY PROFILE	ETHERNET PROFILE	AUTO-SYNC
ap_template		Radio_1_bgn_profile					On
LAG						Enable_lag	On

The *Device Administration* group which is one of the classified form of AP Group (refer “*AP Group Inventory*” on page 219 for further information on AP Groups) is applied to the device settings such as Radio and Connectivity Profiles.

When a AP Template is applied to *Device Administration group*, the Radio Profiles and Connectivity Profiles which are a part of the AP Template will be downloaded on all APs in the Device Administration group.



An AP Template cannot consist of two radio profiles for the same interface.

Before creating the AP Template, independent *Radio Profile* and *Connectivity Profile* must be created. These Radio and Connectivity profiles are applied to the AP Template.

To create independent *Radio Profile* and *Connectivity Profile*. Navigate to Configuration > Profiles > Radio Profile and Connectivity Profile. See “*Add a Radio Profile*” on page 151 and “*Add Connectivity Profile*” on page 154.

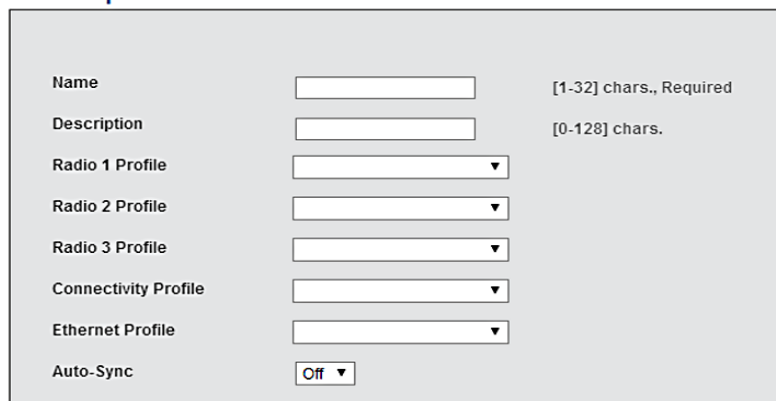
Creating and Applying an AP Template

To create a AP Template, follow these steps:

1. Navigate to *Configuration > Templates > AP Template*.
2. In the *AP Template* screen, select the Add option. The *AP Template - Add* screen is displayed. [Figure 51 on page 149](#) illustrates the *AP Template - Add* screen.

Figure 51: *AP Template - Add*

AP Template - Add



The screenshot shows the 'AP Template - Add' configuration screen. It contains the following fields and controls:

- Name:** A text input field with a character limit of [1-32] chars., Required.
- Description:** A text input field with a character limit of [0-128] chars.
- Radio 1 Profile:** A dropdown menu.
- Radio 2 Profile:** A dropdown menu.
- Radio 3 Profile:** A dropdown menu.
- Connectivity Profile:** A dropdown menu.
- Ethernet Profile:** A dropdown menu.
- Auto-Sync:** A toggle switch currently set to 'Off'.

3. In the *AP Template - Add* screen, provide the details for *Name* and *Description*.
4. Select the *Radio Profile*, *Connectivity Profile* and *Auto-Sync* options from the drop-down list. To add independent Radio, Connectivity, and Ethernet profiles, See [“Add a Radio Profile” on page 151](#) and [“Add Connectivity Profile” on page 154](#).
5. Select Save. The new AP Template is included and is displayed on the *AP Template* screen.

See the **AP Template** screen in Online Help for detailed information on *AP Template* topic.

Updating an AP Template

1. Navigate to *Configuration > Templates > AP Template*.
2. In the *AP Template* screen, select an *AP Template* and select *Edit*. [Figure 52 on page 150](#) illustrates the *AP Template - Update* screen. The *AP Template - Update* screen is displayed.

Figure 52: AP Template - Update

AP Template: LAG - Update

The screenshot shows the 'AP Template' configuration page with the 'Registered Device Groups' tab selected. The page displays various configuration fields for the LAG template:

- Name***: LAG
- Description**: New LAG Configuration [0-128] chars.
- Radio 1 Profile**: Radio_1_bgn_profile
- Radio 2 Profile**: Radio_2_ac_profile
- Radio 3 Profile**: Radio_3_an_profile
- Connectivity Profile**: L3DHCP
- Ethernet Profile**: Enable_lacp
- Auto-Sync**: On

3. The *AP Template - Update* screen displays the following tabs:

AP Template

- The *AP Template - Update* screen provides the *Description*, *Radio Profile*, *Connectivity Profile* and *Auto-Sync* options that can be modified. [Figure 52 on page 150](#) illustrates the *AP Template - Update* screen.

Registered Device Groups

- The *AP Template - Registered Device Groups* screen displays a list of the *Device Groups* registered to the *AP Template*. Only the *Device Administration* group which is one classified form of an AP Group can be registered to the AP Template. [Figure 53 on page 150](#) illustrates the *Registered Device Groups* screen.

Figure 53: Registered Device Groups

Registered Device Groups

AP Template Registered Device Groups Radio Profile Connectivity Profile						
↻ +						
DE VICE GROUP	AVAILA BLE VERSION	APPLIED VERSION	APPLIED TIME	APPLIED STATUS	APPLIED DETAILS	CURRENT STATUS
<input type="checkbox"/> kredum	1	1	11/19/2013 12:16:35	Failed	Failed to apply AP template on one or more APs	One or more APs not in sync with NMS Configuration

- The Registered profiles can be *Force-synced*. The following are the types of Sync status:
 - *In-Sync*: The In-Sync status is displayed if the AP Templates are successfully applied to all Device Groups.
 - *Sync Pending*: The Sync Pending status is displayed, when the auto-sync flag for the AP Template is off and the current version of the AP Template is different from the synced version of the AP Template.

- *In sync with another template*: The In sync with another template status is applicable for nested AP Groups. Where one main group and a sub group are registered to different AP Templates. While viewing the sync details of the Main Group, the sync status for all APs under the sub group is displayed as In Sync with Other Template as the sub group is registered to another AP Template.
- *Failed*: The Failed status is displayed if the AP Template is synced to the Device Groups.

Radio Profile

The *Radio Profile* screen allows you to view the details of the *Radio Profile* applied to the respective AP Template.

Figure 54 on page 151 illustrates the *AP Template - Radio Profile* screen.

Figure 54: AP Template - Radio Profile

Radio Profile

AP Template		Registered Device Groups		Radio Profile	Connectivity Profile
<div><div></div><div></div></div>					
<input type="checkbox"/>	RADIO PROFILE NAME	INTERFACE INDEX	PRIMARY CHANNEL	RF BAND SELECTION	MESH SERVICE ADMIN STATUS
<input type="checkbox"/>	Radio_1_bgn_profile	1	6	802.11bgn	Disable
<input type="checkbox"/>	Radio_2_an_profile	2	36	802.11an	Disable
<input type="checkbox"/>	Radio_3_an_profile	3	149	802.11an	Disable

Connectivity Profile

The *Connectivity Profile* screen allows you to view the details of the Connectivity Profile applied to the respective AP Template.

Figure 55 on page 151 illustrates the *AP Template - Connectivity Profile* screen.

Figure 55: AP Template - Connectivity Profile

Connectivity Profile

AP Template			Registered Device Groups			Radio Profile			Connectivity Profile				
<input type="checkbox"/>	CONNECTIVITY PROFILE NAME ▾					IP CONFIGURATION ▾				DISCOVERY PROTOCOL ▾			
<input type="checkbox"/>	L2NOIP					No IP				L2 preferred			

Add a Radio Profile

An AP comprises of either two or three radios. Each Radio Profile can be configured individually via the controller or *NM*. A radio profile comprises of the configuration parameters which is applied on the wireless interface of the AP. To create independent radio profiles, follow these steps:

1. Navigate to *Configuration > Profiles > Radio > Add*.

2. In the *Radio Profile - Add* screen, provide the details for *Radio Profile Name*, *Interface Index*, *Primary Channel*, *RF Band Selection*, *Short Preamble*, *Transmit Power High (dBm)*, *AP Mode*, *Protection Mechanism*, *Protection Mode*, *Channel Width*, *MIMO Mode* (*MIMO mode is not supported in 8.3 release*) and other options. [Figure 56 on page 152](#) illustrates the *Radio Profile - Add* screen.

Figure 56: Radio Profile - Add

Radio Profile - Add

Radio Profile Name	<input type="text"/>	[1-32] chars., Required
Interface Index	1 ▼	
Primary Channel	<input type="text"/>	
RF Band Selection	802.11b ▼	
Short Preamble	On ▼	
Transmit Power High(dBm)	<input type="text"/>	
AP Mode	Service/Normal Mode ▼	
Protection Mechanism	One-Frame Protection ▼	
B/G Protection Mode	Auto ▼	
HT Protection Mode	Off ▼	
Channel Width	40 MHz Extension channel above ▼	
MIMO Mode	2x2 ▼	
802.11n only mode	Off ▼	
RF Virtualization Mode	Virtual Port ▼	
Probe Response Threshold	15	Valid range: [0-100]
Mesh Service Admin Status	Disable ▼	
Transmit Beamforming Support	Off ▼	
STBC Support	Off ▼	

3. Select Save. The new *Radio Profile* is included and is displayed on the *Radio Profile* screen.

See the **Radio Profile - Add** screen in the Online Help for detailed information on *Radio Profile* topic.

Update the Radio Profile

1. Navigate to *Configuration > Profiles > Radio > select a radio profile by selecting a check box > Edit*
2. In the *Radio Profile - Update* screen, modify the *Primary Channel*, *RF Band Selection*, *Short Preamble*, *Transmit Power High (dBm)*, *AP Mode*, *Protection Mechanism*, *Protection Mode*, *Channel Width*, *MIMO Mode* and other options. [Figure 57 on page 153](#) illustrates the *Radio Profile - Update* screen.

Figure 57: Radio Profile - Update

Radio Profile - Update

Radio Profile Name	Radio_1_bgn_profile
Interface Index	1
Primary Channel	6
RF Band Selection	802.11bgn
Short Preamble	On
Transmit Power(EIRP)	20
AP Mode	Service/Normal Mode
Protection Mechanism	One-Frame Protection
B/G Protection Mode	Auto
HT Protection Mode	Auto
Channel Width	20 MHz
MIMO Mode	3x3
802.11n only mode	Off
RF Virtualization Mode	Virtual Port
Probe Response Threshold	15
	Valid range: [0-100]
Mesh Service Admin Status	Disable
Transmit Beamforming Support	Off
STBC Support	Off
DFS Fallback Option	Disable
DFS Fallback Channel	1
DFS Channel Revertive(minutes)	30
	Valid range: [30-1440]

3. Select **Save**. The updated Radio Profile is included and is displayed on the *Radio Profile* screen.

See the **Radio Profile - Update** screen in the Online Help for detailed information on *Radio Profile* topic.

Add Connectivity Profile

A *Connectivity Profile* comprises of AP configuration parameters related to Network Connectivity. Profiles can be created and applied to a set/group of APs from the NM server. To create independent Connectivity profiles, follow these steps:

1. Navigate to *Configuration > Profiles > Connectivity > Add*.
2. In the *Connectivity Profile - Add* screen, provide the details for *Connectivity Profile Name*, *IP Configuration*, *Discovery Protocol*, *Controller Address* and *Controller Host Name* box.
[Figure 58 on page 154](#) illustrates the *Connectivity Profile - Add* screen.

Figure 58: Connectivity Profile - Add

Connectivity Profile - Add

Connectivity Profile Name	<input type="text" value="Test"/>	[1-32] chars., Required
IP Configuration	<input type="text" value="No IP"/>	
Discovery Protocol	<input type="text" value="L2 preferred"/>	
Controller Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	
Controller Host Name	<input type="text"/>	[0-63] chars.

3. Select **Save**. The new Connectivity Profile is included and is displayed on the *Connectivity Profile* screen.

See the **Connectivity Profile - Add** screen in Online Help for detailed information on *Connectivity Profile* topic.

Update the Connectivity Profile

1. Navigate to *Configuration > Profiles > Connectivity > select a Connectivity Profile by selecting a check box > Edit* option.
2. In the *Connectivity Profile - Update* screen, modify the *Connectivity Profile Name*, *IP Configuration*, *Discovery Protocol*, *Controller Address* and *Controller Host Name* box.
[Figure 59 on page 155](#) illustrates the *Connectivity Profile - Update* screen.

Figure 59: Connectivity Profile - Update

Connectivity Profile - Update

Connectivity Profile Name	Conn_227		
IP Configuration	DHCP ▾		
Discovery Protocol	L3 preferred ▾		
Controller Address	172	19	43 , 227
Controller Host Name	<input type="text"/>		[0-63] chars.

3. Select Save. The updated Connectivity Profile is included and is displayed on the *Connectivity Profile* screen.

See the **Connectivity Profile - Update** screen in Online Help for detailed information on *Connectivity Profile* topic.

APs Not In Sync With NMS Configuration or Mismatched APs

The APs are considered to be in *Mismatched* state when the radio or connectivity configuration present on the controller for the AP is not same as the radio or connectivity configuration which was applied from the *FortiWLM* for that AP. The sync status a modified AP is displayed as *Not in sync with Controller* on the *FortiWLM* server.

The *Mismatch APs* icon is available on the *FortiWLM* screen's *Status bar*, which when clicked is redirected to *APs Not In Sync With NMS Configuration* screen providing a list of APs with the configuration mismatch displayed along with the time stamp when the mismatch was detected.

1. Navigate to on *Configuration > Device View > Mismatched APs* or select the *Mismatch APs* icon that is available on the *FortiWLM* screen's *Status bar*.
2. The *APs Not In Sync With NMS Configuration* screen is displayed providing the *Name*, *MAC Address*, *Device Group*, *Controller*, *Applied Template*, *Difference* and *Review Status* details along with the *Mismatch* details.
3. The *Mismatch* details wizard provides the mismatch configuration details of the AP Template (Radio Profile and Connectivity Profile).
4. The details displayed on the *Mismatch Details* wizard must be acknowledged by selecting the below options:
 - Reviewed/Acknowledged

- Reviewed
5. Once the mismatch is acknowledged, the mismatch will be excluded from the count displayed on the *Status bar*. Select *Close*.

See the **APs Not In Sync With NMS Configuration** screen by selecting the *Mismatched APs* link in Online Help for a detailed information on *Mismatched APs* topic.

Service Control

Fortinet's *Service Control* feature is designed to allow clients in the enterprise network to access and communicate with devices that are advertising service via a protocol such as Bonjour. *FortiWLM* manages multiple controllers and AP groups. The *NM* has the ability to create global settings for the *services*, *create policy templates*, and *create global controller configuration*. One of the major features of this product is the ability to create a *Global Controller Configuration* from *NM* and download it to one or more managed controllers. These *Global Controller Configurations* are owned by *NM* (nms-server) and cannot be altered by the controllers using them. *NM* can download a *Global Controller Configuration* to one or all managed controllers. If you change a *Global Controller Configuration*, all controllers using it are automatically updated with those changes.

The limitation for Bonjour-enabled devices is that they were largely designed for small-scale use; however, they are growing increasingly prevalent in the enterprise-level environment. The nature of the service makes scaling for larger deployments challenging because the wireless traffic communications for these protocols cannot travel across various subnets; as such, users on VLAN1 will be unable to access a device operating on VLAN2 (for example).

Service Control addresses this problem by providing a framework by which Fortinet will direct traffic from clients on different subnets over to the Bonjour-capable devices (and vice versa), allowing seamless communication between the two. Additionally, you can specify which services should be available to specific users, SSIDs, or VLANs, allowing a fine control to be exercised over the deployment.

To enable Service Control:

1. Navigate to *Configuration > Templates > Service Control*. By default, you land on the *Service Control Settings*.

Figure 60 on page 157 illustrates the *Service Control Settings* screen.

Figure 60: Service Control Settings

ServiceControl Settings ⓘ		
Controller Configuration		
List of controllers for which ServiceControl configuration can be modified directly on the controller. Configuration changes from this page are done on running configuration of controller.		
<div>REFRESH ENABLE DISABLE</div> <div>1 - 100 of 107</div>		
CONTROLLER NAME ⓘ	IP ADDRESS ⓘ	SERVICE CONTROL STATUS ⓘ
10.35.5.19	10.35.5.19	Disable
10.35.5.18	10.35.5.18	Disable
10.35.5.52	10.35.5.52	Disable
10.35.5.53	10.35.5.53	Disable
10.35.5.4	10.35.5.4	Disable
10.35.5.5	10.35.5.5	Disable

2. Click the *Global Settings* tab.
3. Check *Enable Service Control*. The page will automatically refresh. Refer to the sections below for configuration instructions.

Modifying Service Control Global Configuration

Once Service Control has been enabled, the *Global Settings* tab displays two new tables: [Figure 61 on page 158](#) illustrates the *Service Control Settings - Global Settings* screen.

- Discovery Criteria*: The discovery criteria allows you to specify the types of services that may be discovered. By default, all *AppleTV* and *Printer* services configured in the system will be set for discovery across all SSIDs and APs and on Controller native VLAN by controller on the wired side. To modify this, click the pencil icon under the Services column to access the *Discovery Criteria* dialog. [Figure 62 on page 158](#) illustrates the *Discovery Criteria* screen.
- Advanced Options*: The Advanced Options will allow you to specify the IP addresses to block the bonjour services.

Figure 61: Service Control Settings - Global Settings


Service Control Settings

Controller Configuration > 172.19.43.251

Global Settings
Services
Locations
User Groups
Policies

☒ **Enable Service Control**
This will enable Bonjour Service Discovery by the system as per below Discovery Criteria.
It will also enforce Bonjour Service Advertisement as per the configured ServiceControl Policies.

Discovery Criteria

Services	Wireless Network		Wired Network	
	SSIDs	Locations	VLANs	Wired Gateway List
 All Services	All SSIDs	All APs	0	Controller

Advanced Options

Blocked Bonjour Gateway List

Bonjour packets from below ip address list will be dropped. You can use these list to ignore Bonjour services from certain ip addresses.
For example, If you have multiple controllers in network, you can add ip address of other controllers in below list, so Services discovered by those controllers will not be re-learned here. This will not affect Bonjour mechanism on other controllers.

☐ NAME
IP ADDRESS

No Data available

EDIT
DELETE

Figure 62: Discovery Criteria

ServiceControl Settings ?

Controller Configuration > 10.35.5.19

Global Settings

Services

Locations

User Groups

Policies

☒ Enable ServiceControl
 This will enable Bonjour Service Discovery. It will also enforce Bonjour Service Discovery.

DISCOVERY CRITERIA

Services

☒ All Services

ADVANCED OPTIONS

Blocked Bonjour Gateway List

Bonjour packets from below ip address
 For example, If you have multiple

☐ NAME

No Data available

REFRESH

ADD

Discovery Criteria

SELECT SERVICES

☒ All services
 AppleTV
 Chromecast
 Printer

SELECT WIRELESS NETWORK

☒ All SSIDs
☒ All APs

SELECT WIRED NETWORK

VLAN List

0

Example 1-3,5

Wired Gateway List

0

ADD

SAVE

CANCEL

1. As shown above, the *All Services* box is checked, ensuring that all configured services will automatically be detected by the system. Uncheck this box and select the desired service(s) if you wish to restrict the types of services provided.
2. The *Select Wireless Network* section allows you to customize which SSIDs/APs can access the services; by default, all of them are permitted.

Templates

159

3. The *Select Wired Network* section controls how wired devices access the services; enter the VLAN(s) that should be allowed access. To add wired gateways, click the **Add** button and specify the desired options from the resulting list of devices.



For Controller to detect services on a tagged VLAN (say VLAN XX), Controller should have a VLAN profile VLAN XX (configured VLAN).

4. Click *Save* to save your changes.

Adding or Removing Services

The Services tab allows you to modify the services that may be detected via Service Control; by default, several services are preconfigured in the system. However, you can expand this list by clicking the *Add* button to create a new service.

Figure 63 on page 161 illustrates the *Add Service* screen.

Figure 63: Add Service

The screenshot displays the 'ServiceControl Settings' page. At the top, there's a breadcrumb 'Controller Configuration > 10.35.5.19'. Below this are tabs for 'Global Settings', 'Services', 'Locations', 'User Groups', and 'Policies'. The 'Global Settings' tab is active, showing a checkbox for 'Enable ServiceControl' which is checked. Below this is a section for 'DISCOVERY CRITERIA' with a table for 'Wireless Network' containing columns for 'Services', 'SSIDs', and 'Locations'. A modal dialog titled 'Add Blocked Gateways' is open, with an arrow pointing to the 'ADD' button. The dialog has fields for 'Name*' (with a character limit of [1-32] chars), 'Description' (with a character limit of [0-64] chars), and 'IP Address' (with a 'Required' label). At the bottom of the dialog are 'CANCEL' and 'SAVE' buttons. Below the dialog, there's a table with a 'NAME' column and a 'No Data available' message.

Fill in the required fields as described below:

- **Name**—Enter a name for the service
- **Description**—Enter a brief description
- **Service Type**—Enter the service type string(s). If multiple entries are needed, enter them one at a time, clicking **Add** after each one. They will display in the *Added Service Types table*.



To remove an added service, verify the box alongside it and click *Delete*.

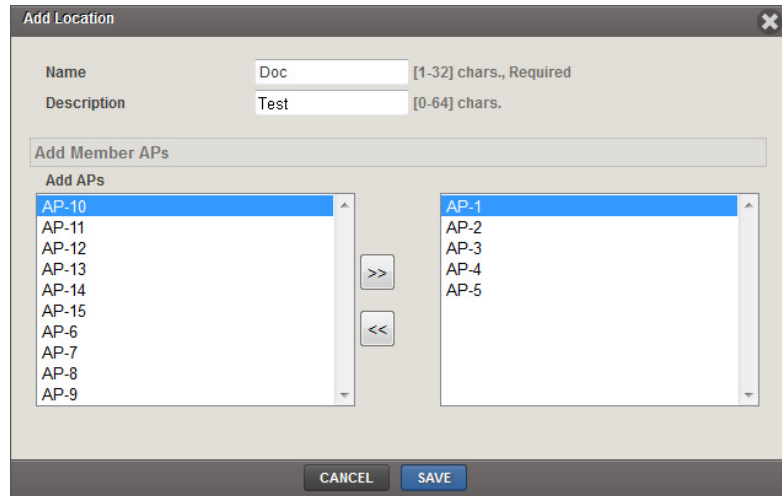
- Click **Save** to save the new service.

Configuring Locations

The *Locations* tab allows you to specify locations where services should be advertised; by default, no locations are configured, so click *Add* to create one.

Figure 64 on page 162 illustrates the *Add Location* screen.

Figure 64: *Add Location*



A Location consists of three main components: the location's name, description, and member APs. Enter the *Name* and *Description* in the fields provided, then select the AP(s) that belong to the desired location from the drop-down list. Click the button pointing to the right to add the selected AP(s) to the new location.

Click *Save*, to view the new location in the *Location Table*. The AP(s) specified in the location definition will now provide access to the service.

Creating User Groups

User Groups segregates Subscriber and Advertisers under a group. User Groups define which users/Advertisers (grouped by either VLAN for wired clients or SSID/Location for wireless) can access the advertised service or advertise the services.

Figure 65 on page 163 illustrates the *Add User Group* screen.



By default, there is no User Group.

Figure 65: Add User Group

Add User Group

Name: [1-32] chars., Required

Description: [0-64] chars.

Role: ☐ Advertiser ☐ Subscriber ☒ Both
Users in this group can be assigned the role of Advertiser and Subscriber in the Policies.

User Group Type: ☒ Wireless ☐ Wired

Select Wireless Users

SSIDs:

Locations: ☐ All APs

CANCEL **SAVE**

A *User Group* consists of four main components: the group's *name*, *description*, *Role*, *User Group Type*, and *SSIDs*. These fields will allow you to customize which users can access the defined services.

1. Enter the *Name* and *Description* in the fields provided.
2. Select one of the *Role* for the user group. The options is Advertiser, Subscriber, or Both.
3. Select the *User Group Type*. The options is *Wireless* or *Wired*.
4. If you have selected *Wireless* user group type, then *Select Wireless Section*. From the *Select Wireless Users* section, select the *SSIDs* that should be allowed access. To select multiple options, click and drag across them. Ctrl+click to select or de-select items individually.
5. If you have selected *Wired* user group type, then the *Select Wired Users* section. Enter the VLAN(s) that should be allowed to access advertised services.
6. Click *Save* to create the group. The devices contained within the group's parameters will now be able to access the advertised services.

Defining Service Control Policies

Service Control policies determine which user groups can access specific advertised services. Thus, the policies table allows you to define routes between the subscriber (i.e., the device that seeks the service) and the advertiser (i.e., the device that provides access to the service).

Figure 66 on page 164 illustrates the *Create Service Control Policy* screen.

Figure 66: *Create Service Control Policy*

The screenshot shows a window titled "Create Service Control Policy". At the top, there is a "Policy Name" field containing the text "Doc" and a label "[1-32] chars., Required". Below this, the window is divided into three main sections. The first section, "Select Subscriber", contains a "User Groups" dropdown menu. The second section, "Choose Services", contains a checkbox labeled "All services" and a list box showing "AppleTV" and "Printer". The third section, "Select Advertiser", contains a "User Groups" dropdown menu. At the bottom of the window, there are two buttons: "CANCEL" and "SAVE".

1. From the *Policies* tab, click *Add* to access the *Create Service Control Policy* window.
2. Enter a name for the policy to be created in the *Policy Name* field.
3. Enter the description of the policy.
4. Use the *Select Subscriber* drop-down to specify the group that should be granted access.
5. Select the desired services from the drop-down list supplied in the *Choose Services* section. Note that if all services should be included, simply verify the *All services* box.
6. Finally, use the *Select Advertiser* drop-down to select the group that supplies access to the services.
7. Click *Save* to save the new policy.

AP Init Scripts

You can now load AP specific scripts files (for example, AP boot scripts) via FortiWLM and push them to controller APs or AP Groups. The default page shows the list of all scripts and options to push the script to controller APs/AP Groups, edit scripts, import Scripts, and export the script file to be used externally.

<div>Monitor</div> <div>Configuration</div> <div> <div>Templates</div> <div>EzSetup</div> <div>Wireless Service</div> <div>AP Template</div> <div>AP Init Script</div> <div>ServiceControl</div> <div>Port Profile</div> </div>	AP Init Script ?				
	<div>REFRESH</div> <div>ADD</div> <div>IMPORT</div>				
	NAME	DESCRIPTION	AP SYNC STATUS	LAST MODIFIED TIME	ACTION
	<input type="text"/>				
	<div>Upgrade2</div>	AP Group push	2/2	11/22/2016 17:31:40	<div>→</div> <div>↺</div> <div>✎</div> <div>🗑</div> <div>📎</div>
	<div>TESTINFO (1)</div>	import	0/0	11/22/2016 17:32:40	<div>→</div> <div>✎</div> <div>🗑</div> <div>📎</div>
	<div>Upgrade1</div>	test	4/4	11/22/2016 17:32:53	<div>→</div> <div>↺</div> <div>✎</div> <div>🗑</div> <div>📎</div>
<div>1 - 3 of 3</div>					

To add a new script, click the ADD button. In the pop-up box, enter a name for the script and provide the script.

AP Init Script ?

REFRESH

ADD

IMPORT

NAME

Upgrade2

TESTINFO (1)

Upgrade1

Name

Description

Script

SAVE

CANCEL

Alternatively, you can load AP Init scripts by importing script files (*.scr), by clicking the IMPORT button.

Port Profiles

You can now create port profile and push them to available ports in access points managed by FortiWLM. Single Port Profile can be applied only to APs of a single controller, if the profile contains VLAN and/or Radius profile. To apply same port profile to multiple controllers create required VLAN and/or Radius profiles with the same name for all the controllers and select it during Port profile creation

To use this feature, do the following:

Create Port Profile (to include security profile in a port profile, create the security profile before creating port profile)

Push the port profile to available ports.

Creating a Port Profile

To create a port profile, go to Configuration > Port Profile (under Templates) and click the add icon to create a port profile

Add Port Profile

Port Profile Name

[1-32] chars.

Status

Disable

VlanTrunk

Disable

Dataplane Mode

Tunneled

VLAN Name

No VLAN

AP VLAN Policy

No VLAN

AP VLAN Tag

0

[0-4094]

Security Profile Name

No Security Profile

Primary Authentication RADIUS

No RADIUS

Secondary Authentication RADIUS

No RADIUS

MAC Auth Primary RADIUS Profile Name

No RADIUS

MAC Auth Secondary RADIUS Profile Name

No RADIUS

MAC Accounting Primary RADIUS Profile Name

No RADIUS

MAC Accounting Secondary RADIUS Profile Name

No RADIUS

Primary RADIUS Accounting Server

No RADIUS

Secondary RADIUS Accounting Server

No RADIUS

Accounting Interim Interval (seconds)

3600

[600-36000]

Allow Multicast Flag

Off

IPv6 Bridging

Off

IP Prefix Validation

Off

CANCEL

SAVE

Push the Port Profile

Click the push icon to view the Apply Port Profile pop-up. Select the available ports and click the APPLY button.

Port Profile

Enable

Disable

Tunneled







No VLAN

No Security Profile

1/1

03/17/2016 16:35:29

1 - 2 of 2

PORT PROFILE NAME	STATUS	VLANTRUNK	DATA PLANE MODE	VLAN NAME	SECURITY PROFILE NAME	NO. OF AP-INTERFACE	LAST SYNC TIME	ACTION
Clear	Enable	Disable	Tunneled	No VLAN	Clear	0/1	03/17/2016 16:12:56	  
Clear-122	Enable							  

Apply Port Profile

Port Profile Name

Clear-122

AP Group

122

APs

AP	ETHERNET INTERFACE INDEX	MODEL	CONTROLLER NAME
AP-3	2	AP122	172.19.35.201

1 - 1 of 1

CANCEL

APPLY

Controller Configuration

The *Controller Configuration* allows you to take periodic and manual *backups* of the *sys*, *startup* and *running configurations* for all online and managed controllers mapped to the *FortiWLM* application. It also allows you to *import* the controller configuration to nms-server for creating common configuration across multiple controllers.

- “[Backup Controller Configuration](#)” on page 169
- “[Importing a Controller Configuration](#)” on page 173

Backup Controller Configuration

The *Controller Configuration Backup* screen ([Figure 67 on page 170](#) illustrates the *Controller Configuration Backup* screen) allows you to capture periodic and manual backups of the *sys*, *startup* and *running configurations* for all online and managed controllers mapped to the *FortiWLM* application.

This section provides instructions for backing up the controller configuration database. You can manually initiate a backup or schedule regular backups through the *FortiWLM* user interface.

- “[Performing a Manual Backup](#)” on page 169
- “[Scheduling Automatic Backups](#)” on page 171



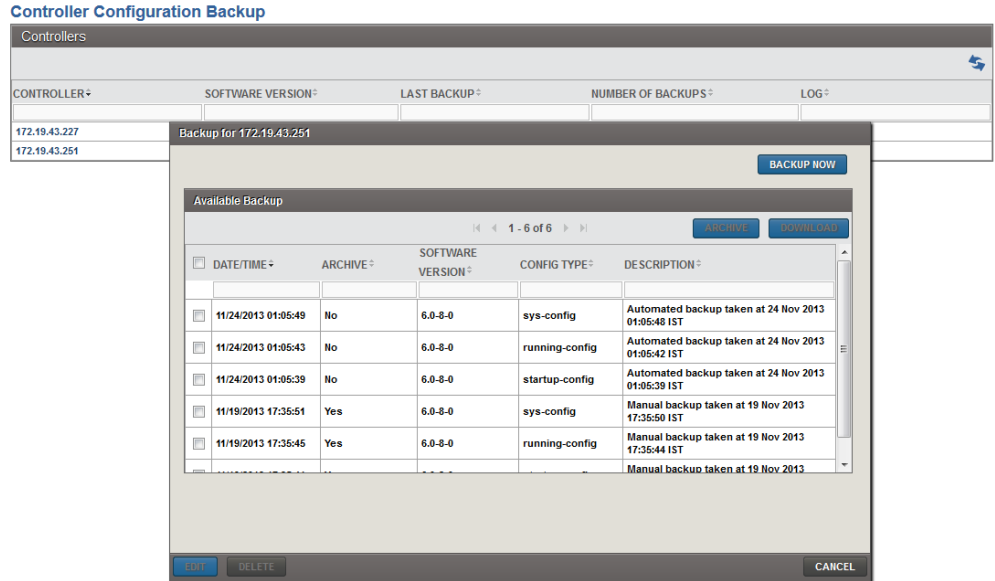
Controller Configuration backups will not be taken for *Slave* controllers.

Performing a Manual Backup

The manual backup creation is based on the role. Only the users possessing configuration capability and scope on a particular controller is allowed to take the controller configuration backup. To back up of the controller configuration database, follow these steps:

1. Log into FortiWLM user interface.
2. Choose *Configuration > Controller Configuration > Backup* to display the *Controller Configuration Backup* screen.
3. The *Controller Configuration Backup* screen summarizes the host name, software version, last backup, number of backups, and log information of each of the controller mapped to the nm server.

Figure 67: Controller Configuration Backup



4. To view the backup details or to perform backup for a selected controller, select the *Controller* link. You can capture periodic backups for all online and managed controllers. The following are the different configurations that can be captured:
 - sys configuration
 - startup configuration
 - running configurations
5. The *Backup History* wizard provides you a complete history of the backup performed for a selected controller with the *Date/Time*, *Archive*, *Software Version*, *Config type*, and *Description* details. You can perform the following actions on the *Backup History* wizard.
 - *Delete*: This option allows you to delete the selected controller configuration backup from the hard disk of the service appliance.



The deletion of the selected controller from the inventory deletes the complete backup data of the related controller.

- *Archive*: This option allows you to archive the selected controller configuration backup on the hard disk of the service appliance.



All the manual configuration backups are archived by default.

- *Download*: This option allows you to download and save the selected controller configuration backup on the computer hard disk in *.tar.gz* format.
 - *Backup Now*: This option allows you to take a backup of the sys, startup, and running controller configurations at the current time interval.
 - *Edit*: This option allows you to edit the description of the selected controller configuration backup.
6. Select the *Detail* link to view the complete history of the backup for the selected controller. The *Backup History* wizard is displayed providing the *Date/Time* of the backup performed along with the *Config Type* and the *Status* of the backup, if failed or passed.

Scheduling Automatic Backups

The data backup is stored in a text format on the nm server. To schedule automatic backups of the controller configuration database, follow these steps:

1. Log into FortiWLM user interface.
2. Choose *Administration > System Administration > Maintenance* to display the *Maintenance* screen. You can modify the controller configuration backup details by navigating to the *Controller Configuration Backup* section of the *Maintenance* screen.
3. The scheduled configuration backup frequency or the *Backup Schedule* is fixed to *Weekly* and cannot be modified.
4. However, you can configure the day of the week for scheduling the weekly configuration backup activity. Modify the default *Backup Day* (Sunday) by selecting a day in a week for the controller configuration backup to be performed. Select any one of the following options:
 - Sunday
 - Monday
 - Tuesday
 - Wednesday
 - Thursday
 - Friday
 - Saturday

- The time scheduled is the server's local time with the default time as 1.00 am. Modify the default *Backup Hour* by selecting a desired time of the day for the backup to be performed from the drop-down list.



In the scheduled backup failure scenario, the backup activity for failed controllers is re-initiated every hour until the backup is successful.

- Click Save to save your settings. The data backup is stored in a text format on the nm server.

Controller Configuration Difference

You can view differences between startup and running configuration of the same controller or two different controllers and apply running-config to startup-config or startup-config to running-config. Select the Controllers and the configuration files to be compared and click **Diff Config**.

Controller Configuration Backup ?

CONTROLLERS

REFRESH DIFF CONFIG BACKUP NOW

CONTROLLER NAME	Configuration 1	Configuration 2
10.34.140.141	Select Controller: 10.34.159.212	Select Controller: 10.34.159.213
10.34.140.143	Select Config file: 09/18/2016 01:05:45(running-config)	Select Config file: 09/18/2016 01:05:54(running-config)
10.34.140.234	Color Definition: Insertion, Deletion	
10.34.143.24	# version 8.1-2-0configure terminalno	# version 8.1-2-0configure terminalno
10.34.159.212	rogue-ap detectionaudit period	rogue-ap detectionaudit period
10.34.159.213	60controller-index 0auto-ap-upgrade	60controller-index 0auto-ap-upgrade
10.34.159.215	enabletopo-update disableaeroscout	enabletopo-update disableaeroscout
10.34.159.216	disableaeroscout ip-address	disableaeroscout ip-address
10.34.159.217	0.0.0.0aeroscout port 12092fastpath	0.0.0.0aeroscout port 12092fastpath
	onclient-handoff-logic onbonding	onclient-handoff-logic onbonding
	single10gig-module	none10gig-module
	disable1gig-sfp disableigmp-snoop state	disable1gig-sfp disableigmp-snoop state
	disableigmp-snoop age-time	disableigmp-snoop age-time
	300roaming-domain stoproaming-domain	300roaming-domain stoproaming-domain
	roam-time-out 60snmp-filter-config	roam-time-out 60snmp-filter-config
	ap-discovered onsnmp-filter-config	ap-discovered onsnmp-filter-config
	ap-assigned offsnmp-filter-config	ap-assigned offsnmp-filter-config
	ap-neighbor offsnmp-filter-config	ap-neighbor offsnmp-filter-config
	ap-neighbor-detail	ap-neighbor-detail
	offstation-aging-out-interval	offstation-aging-out-interval
	2optimization	2optimization
	noneassociated-station-max-idle-period	noneassociated-station-max-idle-period
	2000adequate-signal-threshold	2000adequate-signal-threshold
	-45zeronet-packet	-45zeronet-packet

Importing a Controller Configuration

The *Import Controller Configuration* in FortiWLM assists you to import controller configuration to nms-server for creating a common configuration across multiple controllers. A controller configuration with the available *ESS Profiles* are selected and imported, by performing the actions in the following sequential order:

1. Select *Configuration > Controller Configuration > Import*. The *Import Controller Configuration* screen displays the following sequence of steps:
 - **Select Controller:** The *Select Controller* allows you to import configuration to NMS for creating common configuration for multiple controllers.
 - Select a *Controller* from the drop-down list. Click *Next* to navigate to the *Select Configuration* tab. [Figure 68 on page 173](#) illustrates the *Select Controller* screen.

Figure 68: Select Controller

Import Controller Configuration

The screenshot shows the 'Select Controller' step of the 'Import Controller Configuration' wizard. At the top, a progress bar indicates the sequence: Select Controller (active), Select Configuration, Summary, Review, and Import Status. Below the progress bar, a text box instructs the user to 'Select controllers from where you want to import configuration to NMS server for creating common configuration for multiple controllers.' A dropdown menu labeled 'Controllers' shows '172.19.43.251' selected. A 'NEXT' button is located at the bottom right.

- **Select Configuration:** The *Select Configuration* screen displays a list of available *ESS Profiles*.
 - Select the *ESS Profile* from the *Available ESS Profiles* list and click the *Forward* button. To select multiple options, click and drag across them. Ctrl+click to select or de-select items individually. [Figure 69 on page 173](#) illustrates the *Select Configuration* screen.

Figure 69: Select Configuration

Import Controller Configuration

The screenshot shows the 'Select Configuration' step of the 'Import Controller Configuration' wizard. The progress bar at the top shows: Select Controller, Select Configuration (active), Summary, Review, and Import Status. The main area is titled 'Select Configurations to be imported.' It contains two lists: 'Available ESS Profiles' on the left with 'AP_Lev' listed, and 'Selected ESS Profiles' on the right with 'kreddum-251-bgn', 'kreddum-251-an', and 'ESS_profile' listed. Between the lists are '>>' and '<<' buttons. At the bottom right, there are 'BACK', 'CANCEL', and 'NEXT' buttons.

- Click *Next* to navigate to the *Summary* tab.

- Select *Back* to navigate to the *Select Controller* screen.
- **Summary:** The *Summary* screen displays a summary of selections performed in the *Select Controller* and *Select Configuration* screens. [Figure 70 on page 174](#) illustrates the *Summary* screen.

Figure 70: Summary

Import Controller Configuration

Select Controller
Select Configuration
Summary
Review
Import Status

Following configurations will be imported to NMS server. In the next step you have an option to import only a subset of these and also import these with different names.

ESS PROFILE	ESS PROFILE FOR OVERFLOW	SECURITY PROFILE	PRIMARY AUTHENTICATION RADIUS PROFILE	SECONDARY AUTHENTICATION RADIUS PROFILE	PRIMARY ACCOUNTING RADIUS PROFILE	SECONDARY ACCOUNTING RADIUS PROFILE	VLAN PROFILE	GRE PROFILE	HOTSPOT PROFILE
kreddum-251-bgn		kreddum-2511							
kreddum-251-an		kreddum-2511							
ESS_profile		ESS_profile							

BACK
CANCEL
NEXT

- Click *Next* to navigate to the *Review* tab.
- Select *Back* to navigate to the *Select Configuration* screen.
- **Review:** The *Review* screen allows you to modify the summary of selections performed in the *Select Controller* and *Select Configuration* screens. [Figure 71 on page 174](#) illustrates the *Review* screen.

Figure 71: Review

Import Controller Configuration

Select Controller
Select Configuration
Summary
Review
Import Status

Rename the profiles or exclude profiles which you don't want.

PROFILE NAME	TYPE	NOTE	IMPORT	NEW PROFILE NAME
kreddum-251-bgn	ESS Profile	Profile already exist	<input checked="" type="checkbox"/>	kreddum-251-bgn
kreddum-251-an	ESS Profile		<input checked="" type="checkbox"/>	kreddum-251-an
ESS_profile	ESS Profile		<input checked="" type="checkbox"/>	ESS_profile
kreddum-2511	Security Profile	Profile already exist	<input checked="" type="checkbox"/>	kreddum-2511
ESS_profile	Security Profile		<input checked="" type="checkbox"/>	ESS_profile

BACK
CANCEL
IMPORT

- **Import Status:**
Click *Import*. The *Import Status* screen displays the status of the profiles that was selected to import. [Figure 72 on page 175](#) illustrates the *Import* screen.

Figure 72: *Import*

Import Controller Configuration

Select Controller	Select Configuration	Summary	Review	Import Status
Status of imported configurations.				
PROFILE NAME	TYPE	STATUS		
kreddum-251-bgn	ESS Profile	Import Failed, Profile already exist		
kreddum-251-an	ESS Profile	Imported		
ESS_profile	ESS Profile	Imported		
kreddum-2511	Security Profile	Import Failed, Profile already exist		
ESS_profile	Security Profile	Imported		
				NEXT IMPORT















DHCP Configuration

Configure a DHCP server that can be operated directly from the controller. This configuration is ideal for relatively small deployments that do not require a separate server to handle DHCP duties. This can be particularly useful for deployments that require a DHCP sever for a separate VLAN (such as one used for a guest network) but also would prefer not to allow that traffic to impact the corporate DHCP server.

Creating a DHCP Server

The controller can have multiple different DHCP servers configured on it at any given time. A DHCP server can be associated to only one VLAN. The steps below can be repeated in order to configure different DHCP servers for separate VLANs or Virtual Interface Profiles as needed.

You can now create DHCP configurations from FortiWLM and deploy them to controllers. The default DHCP configuration page, **Configuration > Controller Configuration > DHCP**, lists all online controllers with the IP address. To create DHCP configuration for a controller, select the controller and click the arrow button in the Action column.

DHCP 		
CONTROLLER NAME ²	IP ADDRESS ²	ACTION ²
<input type="text" value=""/>		
10.34.140.141	10.34.140.141	
10.34.140.143	10.34.140.143	
10.34.140.234	10.34.140.234	
10.34.143.24	10.34.143.24	
10.34.159.212	10.34.159.212	
10.34.159.213	10.34.159.213	
10.34.159.215	10.34.159.215	
10.34.159.216	10.34.159.216	
10.34.159.217	10.34.159.217	
  1 - 9 of 9  		

In the resultant page, click **DHCP server** and then click the **Add** button.

DHCP 10.34.140.141

DHCP Lease

DHCP Server

REFRESH

ADD

DHCP SERVER POOL NAME

DHCP Server Pool Name

Enter 1-32 chars.

VLAN Name

No Vlan

State

Enable

Lease Time (in Seconds)

300

Valid range: [300-65535]

IP Pool start

IP Pool End

Domain Name

Enter 0-256 chars.

Primary DNS Server

Secondary DNS Server

Primary Netbios Server

Secondary Netbios Server

DHCP Option 43

Enter 0-32 chars.

SAVE

CANCEL

The following table describes the DHCP server information provided. Note that the table will only be displayed after at least one DHCP server entry has been created.

Option	Description
DHCP Server Pool Name	Enter a name to be ascribed to the DHCP Server.
VLAN Name	This drop-down list allows you to select a VLAN to which the server should be applied. Note that this is only available if the controller is operating in Layer 2 routing mode.
State	Set to Enabled in order to activate the DHCP server, Disabled to deactivate it.

Option	Description
Lease Time	The duration of IP leases that are assigned by the DHCP server. This value is displayed in seconds.
IP Pool Start/End	The start and end IP addresses of the IP pool that may be assigned by the DHCP server.
Domain Name	The domain on which the DHCP server will be active.
Primary/Secondary DNS Server	The primary and secondary DNS servers to be used by the DHCP server.
Primary/Secondary Netbios Server	The primary and secondary Netbios servers to be used by the DHCP server.
DHCP Option 43	Option 43 allows you to manually specify the primary and secondary controllers to be used by the server. Enter the primary and secondary controller IP addresses (separated by a comma) in this field.

Additionally, select the configured DHCP server and click **Delete** to delete the server, click **Settings** to reconfigure the server, and click **View Details** to view a summary of the server configurations.

Mesh Profiles

The Mesh configuration page lists all online controllers. To create a mesh configuration on a controller, click the arrow button in the Action column.

In the resultant page, click the **Add** button to create the Mesh configuration. The Configuration > Wireless > Mesh table describes the current mesh configuration. Note that the table will only be displayed after at least one Mesh network has been created.

- **Name:** Enter a name for the mesh profile.
- **Description:** Enter a brief description for the profile (e.g., its location).
- **Pre-shared Key:** Enter an encryption key for mesh communications. This key will be shared automatically between APs that have been added to the mesh profile; the user will not be required to input it manually later on. This key must be between 8 and 63 characters.
- **Admin Mode:** Setting this field to Enable activates the mesh profile. If the profile needs to be disabled for any reason, set this field to Disable.
- **PlugNPlay Status:** This option allows APs to be added to the mesh by eliminating the need to have them wired connected during mesh configuration.

Deleting the Mesh profile

Select the mesh profile and click **Delete**.

Reconfigure a Mesh profile

Select the mesh profile and click **Settings**. Modify the configuration as required.

Review additional Mesh information

Select the server and click **View Details**. The resulting page displays a quick summary of the mesh configuration.

MAC Filtering

MAC filtering controls a user station's access to the WLAN by permitting or denying access based on specific MAC addresses. A MAC address is unique to each IEEE 802-compliant networking device. In 802.11 wireless networks, network access can be controlled by permitting or denying a specific station MAC address, assigned to its wireless NIC card, from attempting to access the WLAN.

For more information on MAC Filtering, refer to the *FortiWLC Configuration Guide*.

Add MAC Filtering Profile

MAC Filtering Name *

[1-32] chars.

Auto Authentication Expiry Period(Seconds) *

00

:

00

:

20

ACL Allow Access Configuration List

ACL Deny Access Configuration

ADD

DELETE

IMPORT

MAC ADDRESS	DESCRIPTION
<div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div></div>

CANCEL

SAVE

The Wireless LAN System provides MAC filtering using the following methods:

- **ACL Allow Access Configuration List**, which limits access to only those MAC addresses on the permit list

- **ACL Deny Access Configuration**, which specifically disallows access to those addresses (clients) on the deny list

Add addresses to a permit ACL list by specifying them as command arguments, or by importing them from a prepared list. To add one or more MAC addresses to the permit access control list along with a brief description, type the following:

```
controller(config)# access-list permit 00:40:96:51:eb:2b 00:40:96:51:eb:22
controller(config-acl-permit)# descr MyClient
controller(config-acl-permit)# end
```

To import a list of MAC addresses to permit, create a text file listing all the MAC addresses, and import the text file. When creating the text file to be imported, only include one MAC address, in hexadecimal format (**xx:xx:xx:xx:xx:xx**), per line. For example, the contents of a text file to be imported might look like the following:

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
```

After creating the text file, transfer the file to the controller's /images directory. Use the CLI copy command to transfer the file to the controller. Check that the file has been copied using the dir command. The following example shows the command to import a text file named **acl** that adds the MAC addresses to the permit ACL list:

```
controller(config)# access-list permit import acl

00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
00:0c:e6:bd:01:05
```

```
Successfully Added : 7
Duplicate Entries  : 0
Invalid Format      : 0
Entries Processed  : 7
```

To set up a Deny MAC Filtering List, enable the ACL deny state and then either configure a Deny ACL or import a Deny ACL.

A Deny ACL takes precedence over RADIUS Server access, so you can use it to immediately deny access to a station or black-list certain clients (for example, if they have a virus or are attacking other devices).

By default, MAC filtering is disabled. To change the state of MAC filtering so that the deny list is enabled, use the `mac-filter-state deny` command.

Add client addresses to a deny ACL list by either specifying them as command arguments, or by importing them from a prepared list. This command specifies them as command arguments and enters a brief description:

```
controller(config)# access-list deny 00:40:96:51:eb:2b 00:40:96:51:eb:10
controller(config-acl-deny)# descr DenyStation
controller(config-acl-deny)# end
controller(config)#
```

To import a list of MAC addresses to deny, create a text file listing all the MAC addresses, and import the text file. When creating the text file to be imported, only include one MAC address, in hexadecimal format (`xx:xx:xx:xx:xx:xx`), per line. For example, the contents of a text file to be imported might look like the following:

```
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
```

After creating a text file for import, transfer the file to the controller's /images directory using the CLI copy command. Ensure that the file has been copied using the dir command. Then, import the file.

The following example imports a text file named `denyacl` that adds the MAC addresses to the deny ACL list:

```
controller(config)# access-list deny import denyacl
00:04:23:87:89:71
00:06:25:a7:e9:11
00:07:e9:15:69:40
00:0c:30:be:f8:19
00:0c:e6:09:46:64
00:0c:e6:12:07:41
```

```
Successfully Added : 6
Duplicate Entries  : 0
Invalid Format      : 0
Entries Processed  : 6
```

Note:

Active connections do not get disconnected if the ACL environment is changed from Permit to Deny. However, during successive connection the MAC entry is filtered against deny or permit list.

Guest Users

You can add profiles with a list of guest users that can connect via captive portal based as per the rule defined for the guest user profile.

The guest user profile specifies the total time that the guest users can be connected to your network.

Guest User Management ?				
REFRESH		ADD		
GUEST USER PROFILE NAME		CONTROLLER(s)	LAST SYNC TIME	ACTION
Q				
✓ guest		1/1	11/22/2016 17:26:11	→ ↺ ✎ 🗑
1 - 1 of 1				

To create a guest user profile, navigate to **Configuration > Controller Configuration > Guest Users** and click the **ADD** button and update the following:

- Guest User Profile Name
- Username and Password for this user.
- Specify the time limit for the user to be connected to your network in Service Start Time and Service End Time.

Click **Save** to complete the process.

Now, assign the guest user profile to a controller. Select the required guest user profile and click the apply arrow icon to specify the controller IP address.

QoS Rules

Quality of Service rules evaluate and prioritize network traffic types. For example, you can prioritize phone calls (VoIP) or prioritize traffic from a certain department (group, VLANs) in a

company.

You can configure the following QoS rules and push them to controllers

Global Parameters and Marking Management Packets

Value configured as global parameters and for Marking Management Packets will take precedence over values configured from FortiWLC-SD. When pushed to controller, these values will override the controller values and will be replaced with the parameters configured from FortiWLM.

QoS and Firewall Rules & QoS Codec Rules

These rules start with ID 6000 to differentiate them from FortiWLC-SD rules. In FortiWLM you can combine multiple rules into a profile and push them to controllers.

QoS and Firewall Rule

2. In the ID field, type a unique numeric identifier for the QoS rule. The valid range is from 0 to 6000.
3. In the Destination IP fields, type the destination IP address to be used as criteria for matching the QoS rule. The destination IP address is used with the destination subnet mask to determine matching.
4. In the Destination Netmask fields, type the subnet mask for the destination IP address.
5. In the Destination Port field, type the TCP or UDP port to be used as criteria for matching the QoS rule. To specify any port, type 0 (zero).
6. In the Source IP fields, type the source IP address to be used as the criteria for matching the QoS rule. The source IP address is used with the source subnet mask to determine matching.
7. In the Source Netmask fields, type the subnet mask for the source IP address.
8. In the Source Port field, type the TCP or UDP port to be used as criteria for matching the QoS rule. To specify any port, type 0 (zero).
9. In the Network Protocol field, type the protocol number of the flow protocol for the QoS rule. The protocol number can be a number 0 through 255. The protocol number of TCP is 6, and the protocol number for UDP is 17. For a list of protocol numbers, see <http://www.iana.org/assignments/protocol-numbers>.
If you are also using a QoS protocol detector, you must match the network protocol with the type of QoS protocol. Use the following network protocol and QoS protocol matches:
 - UDP: SIP
 - TCP: H.323 or SIP
10. In the Firewall Filter ID field, enter the filter-ID to be used (per-user or per-ESS), if Policy Enforcement Module configuration is enabled (optional feature). This ID must be between 1 and 16 alphanumeric characters.

11. In the Packet minimum length field, specify the size of the minimum packet length needed to match the rule. (Valid range: 0-1500.)
12. In the Packet maximum length field, specify the size of the maximum packet length needed to match the rule. (Valid range: 0-1500.)
13. In the QoS Protocol dropdown list, select one of the following:
 - SIP
 - H.323
 - Other
 - None

For capture rules, the QoS protocol determines which QoS protocol detector automatically derives the resources needed for the flow (implicitly). Select Other if you want to specify the resource requirements for matched flows explicitly. The QoS protocol value is ignored for non-capture rules.

14. In the Average Packet rate box, type the average flow packet rate. The rate can be from 0 through 200 packets/second.
15. In the Action list, select the action the rule specifies:
 - Forward: A flow is given an explicit resource request, bypassing the QoS protocol detector and regardless of whether a QoS protocol was specified.
 - Capture: The system, using a QoS protocol detector, analyzes the flow for its resource requirements.
 - Drop: The flow is dropped.
16. In the Token Bucket Rate box, type the rate (in Kbps or Mbps, depending on the option checked) at which tokens are placed into an imaginary token bucket. Each flow has its own bucket, to which tokens are added at a fixed rate. To send a packet, the system must remove the number of tokens equal to the size of the packet from the bucket. If there are not enough tokens, the system waits until enough tokens are in the bucket.
17. In the Priority box, type the priority at which the flow is placed in a best-effort queue. Packets in a higher priority best-effort queue are transmitted by access points before packets in lower-priority queues, but after packets for reserved flows. Priority can be a value from 0 through 8, with 0 specifying no priority and 8 specifying the highest priority. The default value is 0. If you enable priority (specify a non-zero value), you cannot specify an average packet rate or token bucket rate.
18. In the Traffic Control list, select one of the following:
 - On
 - Off
 - For all types of flows (explicit, detected, and best-effort), selecting On for traffic control restricts the flow to the rate you specified. Packets above that rate are dropped.
19. In the DiffServ Codepoint list, select the appropriate DiffServ setting, if applicable.

20. In the QoS Rule Logging list, select whether to enable or disable logging activity for this QoS rule:
- On
 - Off
21. In the QoS Rule Logging Frequency field, change the default collection interval in which packets related to this rule are logged, if QoS Logging is enabled. The interval must be a number between 30 and 60 (seconds).
22. Match Checkbox: For any field with the corresponding Match checkbox selected, the action mentioned in the ACTION field is performed on the matched packets. If the match checkbox is not checked, packets with any value are matched regardless of the data in the field and the action mentioned in the ACTION field is not performed on the packets. Also see [“More About the Match Checkbox and Flow Class Checkbox” on page 375](#).
23. Flow Class Checkbox: Flow Class options are relevant only for Flow Control rules (rules with Traffic Control enabled and Token Bucket Rate specified) and Firewall rules. This is typically rate limiting. When Flow Class is checked for a field, if a packet has matched a rule (either Flow Control or Firewall types), these fields are stored in the Flow Class entry. A Flow Class entry is used by the system for aggregating a set of flows so that they can be subjected to similar behavior, be it dropping the packets, or rate limiting them. For example, if a rule has a Src IP address of 0.0.0.0 and the Flow Class box checked, and Token Bucket Rate set to 10 kbytes/sec, all packets passing through the system must match this rule, and each flow will be allowed a maximum throughput of 10000 bytes/sec. If the rule were to have Src IP address of 10.0.0.10 and the Flow Class box checked, with a Token Bucket Rate of 10 kbytes/sec, all packets coming from a machine with IP address 10.0.0.10, must match this rule, and the cumulative throughput allowed for this machine shall be no more than 10000bytes/sec. Also see [“More About the Match Checkbox and Flow Class Checkbox” on page 375](#).
24. To add the QoS rule, click OK.

Beacon Services

Fortinet Beacon Services use iBeacon to allow mobile application (iOS and Android devices) to receive signals from beacons in the physical world to deliver hyper-contextual content to users based on location. Bluetooth Low Energy (BLE) is the wireless personal area network technology used for transmitting data over short distances. Broadly, the Beacon Service requires a Bluetooth based iBeacon device to broadcast signals and a mobile application to receive these signals once it comes in the configured proximity. You can now create multiple Beacon Service profiles and map APs to a specific profile.

The Beacon services are available by default in FAP U421EV, FAP U423EV, FAP U321EV and FAP U323EV. For other non-wave2 APs, you will need Bluetooth adapters (For example: Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Bluetooth Dongle and logear Bluetooth 4.0 USB Micro Adapter GBU521). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.

Note:

Access points must be connected to 802.3at power supply.

On upgrading the FortiWLM from a previous version to the latest, the existing Beacon profiles in FortiWLM are unregistered from the Controller.

You can perform the following operations to manage the Beacon Services. Navigate to **Configuration > Controller Configuration > Beacon Services**.

Adding Beacon Services Profiles

This option allows you to add a **Beacon Service**. You can create multiple Beacon Service profiles and also map APs to a specific profile.

APs part of a profile send iBeacons that will help advertise hyperlocal content to users in context to their location.

The screenshot shows the 'Add Beacon Services' configuration window. It includes the following fields and controls:

- Name**: Text input with value 'Beacon-Ap-Grp1'. Placeholder: '[1-64] AlphaNumeric chars.'
- Description**: Text input with value 'AP Group PUsH'. Placeholder: '[0-128] chars.'
- Advertise BLE Beacon**: Dropdown menu with value 'Disable'.
- Beaconsing Interval (ms)**: Text input with value '100'.
- Universal Unique Identifier (UUID)**: Text input with value '25449383-0c42-05cf-6061-778735800404'. A red button labeled 'GENERATE UUID' is to the right.
- Major Number**: Text input with value '56'.
- Minor Number**: Text input with value '78'.
- Transmit Power**: Dropdown menu with value '14 (0dBm)'.

At the bottom right, there are two red buttons: 'SAVE' and 'CANCEL'.


- **Name** – Unique name for this **Beacon Service** profile. The supported range is 1-64 alphanumeric characters.
- **Description** – A description of the created Beacon Service. The supported range is 0-128 characters.

- **Advertise BLE Beacon** – Enables the BLE beacons to advertise packets received by devices. These packets determine the location of the device with respect to the Beacon.
- **Beaconing Interval (ms)** – Select the time interval at which the Beacons transmit signals to associated devices, that is, this sets the rate at which beacons advertise packets. Setting the beacon interval to a higher value decreases the frequency of unicasts and broadcasts sent by the AP. The supported range is 100-1000 milliseconds.
- **Universal Unique Identifier (UUID)** – Click **Generate UUID**, to receive a UUID that is specific to the beacon. The purpose of the ID is to distinguish iBeacons in your network from all other beacons in other networks not monitored by you.
- **Major Number** – This number is assigned to some beacons in a network and is used to distinguish this subset of beacons within a larger group of beacons. For example, beacons within a particular geographic area can have the same major number. The supported range is 0 to 65535.
- **Minor Number** – This number is assigned to identify individual beacons. For example, each beacon in a group of beacons with the same major number, will have a unique minor number. The supported range is 0 to 65535.
- **Transmit Power** – Select a power level for the beacon's transmit signal. The higher the power, the greater will be the range of your signal. The supported range is 0 (-29 dBm) to 15 (4dBm).

Enabling Beacon Services Profiles

Select the Beacon Services profile and click  in the **Action** column to enable the profile.

Applying Beacon Services Profiles to APs

Select the **Beacon Services** profile and click  in the **Action** column to apply the profile to specific APs. You can apply the profile to all APs of a Controller or to specific APs. These are the supported options:

- **AP Groups** - Select a group from the drop-down list. The profile is pushed only to the APs in the AP Group.
- **Controller** - Select the Controller from the drop-down list and select the supported APs. The profile is pushed to the selected APs.

×

Apply Beacon Services

Name *

Beacon-5

AP Groups ⓘ *

×Ap-Grp-832

Controller *

×10.34.133.230

×10.33.115.28

Search for AP names..

<input type="checkbox"/>	AP Name	AP Model	Connectivity Type	HostName
<input checked="" type="checkbox"/>	AP-2	AP822i	L3 preferred	10.33.115.28
<input checked="" type="checkbox"/>	AP-4	AP822e	L3 preferred	10.33.115.28
<input type="checkbox"/>	AP-5	AP832e	L3 preferred	10.33.115.28

APPLY


CANCEL

Note: Controller versions 8.3.0 and above are supported. The list of APs is available only in FortiWLM 8.3.3 and later.

Editing Beacon Services Profiles

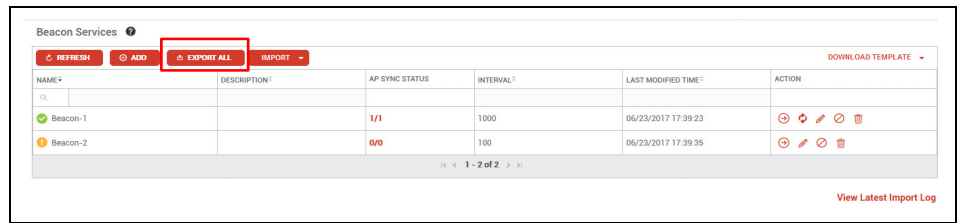
Select the Beacon Services profile and click  in the Action column to edit the values for an existing profile.

Deleting Beacon Services Profile

Select the **Beacon Services** profile and click  in the **Action** column to delete the profile.

Exporting Beacon Services Profiles

You can export the existing Beacon profiles into your local drive.



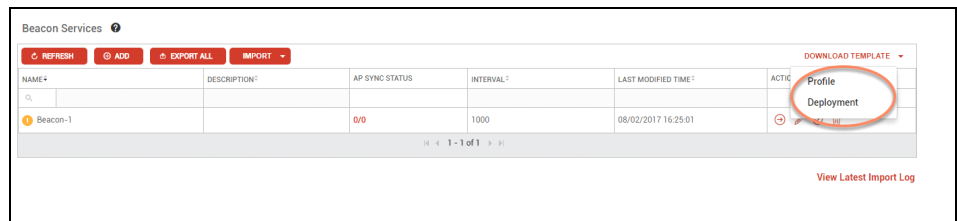
Note:

The **Export All** option exports the Beacon profiles, but does not export the associated APs.

Importing Beacon Services Profiles

You can load Beacon Services profiles by importing files (*.csv) from your local drive.

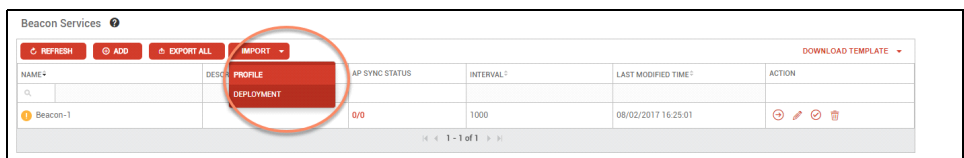
Use the **Download Template** option to download the default **Profile** and **Deployment** templates.



Edit and save these templates.

	A	B	C	D	E	F	G	H
1	name	uniqueidentifier	interval	minnumber	majornumber	descr	blebeacon	transmitpower
2	Beacon-3	545f4426-2896-0785-2c75-97d178e2a613	400	45	56		Enable	-18

Click **Import** and browse to the saved *.csv template file (**Profile** or **Deployment**).



In case of errors, view the import logs using the **View Latest Import Log** option for error details.

	A	B	C
1	name	controllerId	apId
2	Beacon-2	4	1:2:3

View Import Log

PROFILE NAME*	ERROR*
Beacon-3	BEACON Interval can only be in multiples of 100
&^(&***&	Name can only be AlphaNumeric characters
Beacon-5	BEACON UUID Value Invalid
Beacon-6	Minor number can only be an Integer Value and can only range between 0 and 65535
Beacon-7	Major number can only be an Integer Value and can only range between 0 and 65535
Beacon-8	BEACON Flag can only be Disable or Enable
Beacon-9	Transmit Power can only be within these values [4,0,-2,-4,-6,-8,-10,-12,-14,-16,-18,-21,-23,-25,-27,-29]
Beacon-10	Mandatory parameter(s) cannot be Empty

1 - 8 of 8

Select the **Apply Beacon Services** option to apply these to the APs.

Auto Radio Resource Provisioning (ARRP)

ARRP is a mechanism that allows auto selection of channels for optimum use with respect to a given RF environment. By default, in a native cell the administrator manually allocates channels. By enabling ARRP, each AP scans all channels and provides the scan details to the controller. The controller uses this information to select and allocate the best available channel per radio.

By default, this feature is disabled.

- Supported only on 11ac APs.
- Once enabled, the virtual cell is not available for 11ac APs.
- Non-11ac APs will continue to work as configured and will not be affected by auto channel feature.
- The APs will reboot to the newly allocated channel after both initial planning and dynamic channel change.

If the ARRP is disabled, all 11ac APs will reboot to default channels.

Configuring ARRP

To configure ARRP across one or more controllers, create an ARRP profile with required settings and push this profile to one or more controllers.

Automatic Radio Resource Provisioning ?

Add ARRP Profile

ARRP Name * [1-32] chars.

ARRP Status

Radio 1 Planning channel

Radio 1 Planning channel Width

Radio 2 Planning channel

Radio 2 Planning channel Width

Auto Power

Freeze

Timer State

Timer (min) [15-3600]

DFS






- **Planning Channel:** Once enabled, the respective radios of all APs are set to the channels selected for radio 1 and radio 2. In the above screenshot, the planning channel is set to 11 /20MHz for radio 1 and 48/20MHz for radio 2. Based on the report received by all APs, the controller allocates the optimum channel. DFS channels are not available to be set as planning channel
- **Auto Power:** The auto power functionality is applied only after channel allocation irrespective of when the auto power option was enabled. When enabled, the controller will determine the optimum power level between neighbouring (by channel) 11ac APs. The auto power option can be enabled and applied only when ARRP is enabled.
- **Freeze:** The option is applied after the initial planning phase. When this option is disabled, the 11ac APs perform periodic scan (at the end of every minute) on their allocated channels. This is used to determine the quality of the channel. If the quality of the channel crosses the threshold limit (based on three consecutive scans), it sends a request for change of channel. If enabled, the periodic scan is disabled and the 11ac APs remain in

allocated channels irrespective of the channel quality. If this option is disabled, the radio interface settings cannot be modified.

- **Timer State and Timer:** This option is available only when the Freeze option is disabled. To avoid frequent channel change, you can set the channel scan interval to happen at the end of 15 minutes. By default the timer interval is set to 15 minutes and maximum is 3600 minutes. When enabled, the APs start their channel quality scan at the end of 15th minute and continue to scan at the end of every minute for 10 minutes. Based on the data gathered during this period channel change may happen. At the end of the 10 minute of the scan, the channel scanning is disabled for the next 15 minutes.
- **DFS:** By default scanning and allocation of DFS channel is disabled during the planning phase. If enabled, the APs can scan DFS channels and they can be allocated DFS channels. DFS option must be selected when ARRP is enabled. Enabling DFS after enabling ARRP will require re-planning of channel allocation for all APs.
- **REPLAN:** This option is to be used if a new AP is added to the network after the initial planning is complete.

Push ARRP Profiles

Click the profile push icon to push the profile to 1 or more managed controllers.

Automatic Radio Resource Provisioning ⓘ										
ARRP PROFILE NAME*	ARRP STATUS*	RADIO 1 PLANNING CHANNEL*	RADIO 2 PLANNING CHANNEL*	AUTO POWER*	FREEZE*	TIMER STATE*	TIMER (min)*	DFS*	REGISTERED CONTROLLERS*	ACTION*
 testing	Disable	6	36	On	No	Off		Off	1/1	   
1 - 1 of 1										

Other options include:

- **Force Apply:** Click the force apply icon to push the profile again to the controllers or to specific static AP Groups.
- **Replan:** Click the replan icon to restart ARRP planning.

Limitations

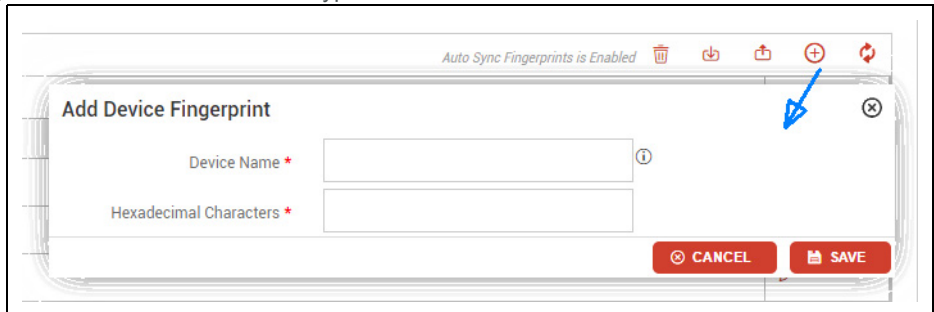
If disabled, existing vCell profiles will be pushed to all 11ac APs irrespective of whether the AP was part of the vCell profile before auto channel feature was enabled. Native cell profiles will remain unchanged.

Device Fingerprinting

You can manage device OS fingerprinting options (configuration and monitoring) from the WebUI. The options include:

- Adding a new device OS type
- Importing Device OS type list
- Export device OS type list
- Editing an existing device OS type
- Deleting an existing device OS type

Add a new device OS type: Click the add icon and enter the device name and the corresponding hexadecimal value of its OS type.



Auto Sync Fingerprints is Enabled

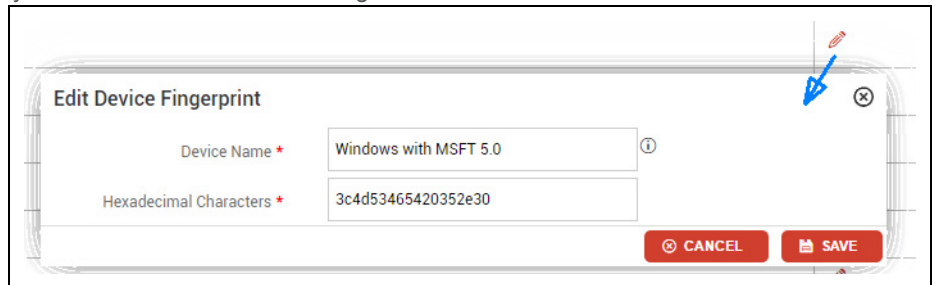
Add Device Fingerprint

Device Name *

Hexadecimal Characters *

CANCEL SAVE

Edit an existing device OS type: Click the edit icon in the action column of corresponding the entry to be modified and made changes.



Auto Sync Fingerprints is Enabled

Edit Device Fingerprint

Device Name *

Hexadecimal Characters *

Windows with MSFT 5.0

3c4d53465420352e30

CANCEL SAVE

Export entries: Click the export icon to export full or selected list of entries to a text file. This can then be imported to another server. To export specific entries, select the checkbox against the entries and click the export icon.

The screenshot shows the 'Device Fingerprint' interface. On the left is a sidebar with navigation options: Monitor, Configuration, Templates, Wireless Service, AP Template, ServiceControl, Port Profile, Device View, Controllers Conf, Mismatched APs, Device Fingerprint (highlighted), Mobility Domain, Inventory, Report & Notif, Visualization, and Administration. The main area has two tabs: 'Device Fingerprint' (active) and 'Device Fingerprint Sync Status'. Below the tabs is a table with columns: DEVICE NAME, HEXADECIMAL CHARACTERS, and ACTION. The table contains several entries for Apple iOS, Apple Mac OS X, and Ascom devices. A blue arrow points from the 'Device Fingerprint' tab to the 'Export' icon (a document with an arrow) in the top right of the table.

DEVICE NAME	HEXADECIMAL CHARACTERS	ACTION
Apple iOS	370103060f77fc	[Edit]
Apple iOS 9.x	37017903060f77fc	[Edit]
Apple Mac OS X 10.6-	370103060f775ffc2c2e2f	[Edit]
Apple Mac OS X 10.7+	370103060f775ffc2c2e	[Edit]
Ascom 2.x Phone	370103060f2c2e2f4243	[Edit]
Ascom 4.x Phone	370103060f2a07642c2e	[Edit]
Ascom i62 Phone	370103060f2a07582c2e	[Edit]
Ascom 5.x Phone	370103060f2a07642c2e2b	[Edit]
Ascom-Myco-phone	37012103060f1c2b333a3b	[Edit]

Import new entries: To import new entries, click the import item and browse to the location that has the text file and click the UPLOAD button.

The screenshot shows the 'Add Device Fingerprint File' dialog box. It has a title bar with 'Add Device Fingerprint File' and a close button. Below the title bar is a text input field with 'Upload File *' and a 'Choose File' button. At the bottom are two buttons: 'CANCEL' and 'UPLOAD'. A blue arrow points to the 'Import' icon (a document with an arrow) in the top right of the dialog.

Delete entries: To delete an entry, select the checkbox of the entry and click the trash can icon.

Duplicate entries are observed in the following cases:

- If a device OS type was edited when one of the managed controllers (previously synced with entries) is offline, re-sync will result in duplicate entries.
- Reset of device fingerprints from WLM after syncing with few edits.

Application Visibility

Fortinet WLM allows you to monitor and/or block traffic based on applications used by clients in your network. By default, FortiWLM allows all application traffic and monitoring data is shown as cumulative value of all usage.

The application visibility feature in FortiWLM allows you to do the following:

- Monitor application traffic
- Block applications
- Create and push policies to controller
- Control bandwidth usage (Bandwidth Throttling)
- Modify priority of application traffic using DSCP values. (DSCP Marking)
- View blocked statistics (Blocked Stats)

To monitor or block applications, you must create application visibility policies. Application visibility will take effect only after the policies are pushed to the controller.

To create a policy, do the following:

1. In the FortiWLM WebUI, go to **Configuration > Application Visibility** to view the DPI Global Configuration page.
2. Policies are defined in the Policy and System Applications section of the page. Click the + icon to create policies in the Add Policy settings window. Enter the following details to create a policy rule:

Figure 73: Add DPI Policy

Add Policy

Policy Name * CorpNet

Description Monitor iTunes and Block Facebook

Policy Status ☒ Enable

Applications

Detect

Block

Controller List

ESSID's for Controllers

- 172.19.44.241
 - ☒ msraju
 - ☐ farida
 - ☐ shai
 - ☐ test
 - ☐ test1

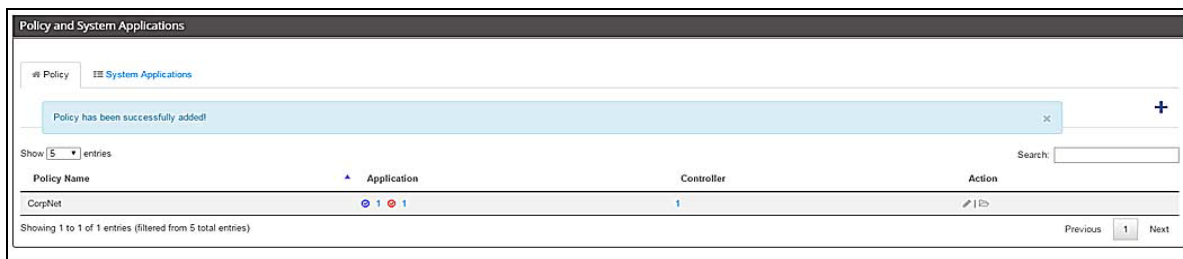
3. Specify a Policy Name to identify the policy
4. Provide Description for the policy.
5. Toggle the Profile Status switch to Enable
6. To add applications for monitor or to block, click either the Detect text box or Block text to view the list of supported application and select the required application. To add more than one application click on the textbox again after adding an application.
7. Select the controller to select the required ESSID and click SAVE to add the policy.



A single policy can be used to monitor and detect applications.

After the policy is added, it is listed in the Policy and System Applications section. For each policy, this section shows the number of applications being monitored (blue color) and blocked (in red color).

Figure 74: DPI Policy Listing



Policy Name	Application	Controller	Action
CorpNet	1	1	

DSCP Marking

DSCP value is selectable field that can be used to assign various levels of precedence to network traffic. By default, traffic packets contained an EF value and with the introduction of DSCP you can now change the priority bit from EF to a DSCP value.

Valid DSCP value strings

- af11
- af12
- af13
- af21
- af22
- af23
- af31
- af32
- af33
- af41
- af42
- af43
- cs0
- cs1
- cs2
- cs3
- cs4
- cs5
- cs6
- cs7

- no
- ef

For more details about DSCP values, see: <https://tools.ietf.org/html/rfc4594>

When a DSCP value is applied to application traffic, this value and the associate priority is maintained till the next node in the traffic. If the traffic carrying the DSCP value encounters a QoS aware switch, then the DSCP value maybe overridden by a QoS value specified by the switch.

Bandwidth Throttling

You can now enforce and allocation maximum bandwidth usage limits for individual applications.

Configuration

To enable bandwidth throttling and mark DSCP value, Go to Configuration > Application Visibility > Policy

ADD POLICY

Policy Name: APV-BWT

Description:

Policy Status: **Enable** (1)

Advanced Detection: **Disable**

Bandwidth Limits: **Enable** (2)

Applications:

Detect: ☒ Facebook ☒ Truphone (3)

Block: Select Applications to Block

Application Name	Client	Bandwidth Limits	SSID	
Facebook	150	Kbps	150	Kbps
Truphone	150	Kbps	150	Kbps

DSCP Value Dropdown: af11, af12, af13, af21, af22, af31, af32, af33, af41, af42, af43, cs0, **cs1**, cs2, cs3, cs4, cs5, cs6, cs7, af22 (5)

1. Enable policy
2. Enable Bandwidth limits

	Minimum	Maximum
Client	150 kbps	1 Gbps
ESSID / Port Profile	150 kbps	12 Gbps

3. Select applications.

4. You can specify maximum limits per client and per SSID
5. In the DSCP Marking column, select the DSCP value.

Blocked Statistics

The application visibility dashboard is enhanced to display visual statistics of blocked traffic. The following screenshots illustrates blocked statistics for blocked applications (Facebook, YouTube, and Skype)

Create a policy

EDIT POLICY

Policy Name: Sun

Description:

Policy Status: **Enable**

Advanced Detection: **Enable**

Bandwidth Limits: **Disable**

Applications: Detect

- Rest All Application
- SKYPE
- Facebook
- YouTube

View blocked Statistics

To view blocked statistics, go to Monitoring > Application Visibility > Blocked tab

# Detected		Blocked			
	APPLICATION NAME	USERS	APS	ESSIDS	UTILIZATION
🟢	YouTube	2	1	2	280 KB
🟢	Facebook	2	1	2	137 KB

Roaming Across Controllers

Clients can roam between access points connected to two different controllers in same subnet or different subnets. System director allows you to specify static or dynamic roaming.

Things to consider before enabling RAC

- IP PREFIX validation has to be OFF in the RAC enabled ESS profile.

- RAC can be enabled on more than one ESSID
- If any parameter of an ESSID profile is changed, then RCA must be stopped and the changes made in the ESSID must be updated to all controllers in the roaming domain.
- Ensure that the controller IP is reachable before adding its IP address to the roaming domain.

In **static DHCP home** configuration, you specify one of the controllers (in the roaming domain) as the home controller. A client associating with any controller in the roaming domain will receive IP address from this home controller. Once a controller is set as home, it applies to all the native VLAN, configured VLAN and dynamic VLAN configurations of that controller as per the "tunnel interface type" set in the ESS profile.

In **dynamic DHCP home** configuration, a client associating with a controller for the first will continue to receive IP address from that controller. This controller will be the home controller for the client. To allow dynamic roaming, set the home controller IP address as 0.0.0.0.

When RAC is stopped all the existing clients are forcefully de-authenticated and forced to reconnect. Irrespective of the client has roamed or not, this process is applied on all clients in the roaming domain.

To configure RAC in FortiWLM, do the following:

1. Specify a Mobility Domain Name
2. Select an ESSID profile (Wireless Service)
3. Select member controllers attached to that ESSID profile. You can select a maximum of 6 controllers as member controllers
4. Select a Home DHCP IP: The IP address of the home controller in the roaming domain. All the DHCP packets from the visiting client will be forwarded to this home controller and will be delivered locally in home.

Add Mobility Domain

Mobility Domain Name * [1-32] chars.

Max 30 controller allowd , Total selected controller: 1

<input type="checkbox"/>	Wireless Service	Member Controllers (Max 6 unique controller can be selected)	Home DHCP IP
<input type="checkbox"/>	wpa2-psk	<input type="text" value="172.19.41.240"/>	<input type="text" value="172.19.41.240"/>

5. Now, click the PUSH icon to push this this profile to selected controllers.

Mobility Domain ?

MOBILITY DOMAIN NAME↕		WIRELESS SERVICE↕	DOMAIN CONTROLLER(s)↕	LAST SYNC TIME↕	ACTION↕
<input type="text"/>					
1 Roam1		wpa2-psk	0/1		<div><div></div><div></div><div></div></div>

5 Monitoring Network Inventory

Devices

The *Devices* in the *Inventory* allows you to

- Discover and manage controllers—“*Controller Inventory*” on page 203
- Manage APs—“*Access Points Inventory*” on page 211
- Discover third party devices—“*Switches*” on page 215

Controller Inventory

FortiWLM manages multiple controllers and access points. You can create from *FortiWLM* and download it to one or more managed controllers. If you modify a , all controllers using it are automatically updated with those modifications. The s are owned by nms and cannot be altered by the controllers using them.

This chapter describes creating and applying s.

Add Controllers to FortiWLM

To add a controller to the *NM* inventory using a supported release, do the following:

1. Navigate to *Inventory > Devices > Controllers*.
2. In the *Controllers* screen, select the *Add* icon. Provide the following details.

Figure 75 on page 204 illustrates the *add controllers* screen.

- **Specify Address:** This option is selected if the controller is behind NAT. The server IP address, which is reachable from controller, must be specified in the *Server IP Address* field.
 - **VPN Server IP Address:** This option is selected
 - **Auto Save Configuration:** This option enables the automatic saving of updates to the Controller configuration.
 - **Server IP Address:** Type the Server IP Address. This option is enabled, only if you want to specify an IP address by selecting the *Specify Address* check box in the *Server Connectivity Preference*.
4. Select *Save*.
 5. The controller is included and is displayed on the *Controllers* screen.

Modify Controllers

Controller Inventory Details - Update

To modify a controller, do the following:

1. Navigate to *Inventory > Devices > Controllers*.
2. In the *Controllers* screen, select a controller by clicking the check box and select the *Edit* option.
3. In the *Controller Inventory Details - Update* screen modify the following fields:
 - **Hostname/IP Address:** Modify the controller's IP address or name.
 - **SSH Port:** Modify the SSH port number. The controller can be added with the user defined port number.
 - **User:** Modify the user ID for the controller.
 - **Password:** Modify the encrypted password for the controller.
 - **Management Administrative State:** Modify the *Management Administrative State*. The possible values are *Managed*, *Deleted*, *Maintenance*, or *Unlicensed*.



License violation message is displayed, when the number of APs exceed the number of Licenses. A grace period of 30 days is provided. After the grace period, the *Management Administrative State* is modified from the default *Managed* state to *Unlicensed*. The *Management Administrative State* is automatically modified to *Managed* after you upgrade the License.

- **Controller Group Name:** Modify the controller group name by selecting a different group name from the drop-down list.
- **Server Connectivity Preference:** Modify the *Server Connectivity Preference* by selecting one of the following options:
 - **User Default:** This option is selected if the controller is in the same sub-network (Not behind NAT).

- **User Server Public IP:** This option is selected to configure the public *IP Address* in *Administration->Server Details->Public IP Address* screen.
 - **Specify Address:** This option is selected if the controller is behind NAT. The server IP address, which is reachable from controller, must be specified in the *Server IP Address* field.
 - **VPN Server IP Address:** This option is selected.
 - **Auto Save Configuration:** This option enables the automatic saving of updates to the Controller configuration.
 - **Server IP Address:** Modify the *Server IP Address*. This option is enabled, only if you want to specify an IP address by selecting the *Specify Address* check box in the *Server Connectivity Preference*.
 - **HTTPS Port:** Modify the HTTPS port number.
4. In the *Controller Inventory Details - Update* screen view the following fields:
- **Communication IP Address:** Displays the controller's IP address.
 - **Network Device Id:** Displays the *Network Device Id* of the controller.
 - **Node Name:** Displays the *hostname* configured on the controller.
 - **Description:** Displays the description provided on the controller.
 - **Location:** Displays the location information configured on the controller.
 - **Contact:** Displays the contact information configured on the controller.
 - **Software Version:** Displays the controller's runtime software version.
 - **Controller Model:** Displays the controller's appliance hardware model such as MC4100 or MC3000.
 - **Availability State:** Indicates whether a controller is reachable or not from *FortiWLM*.
 - Online indicates reachable
 - Offline indicates not-reachable.
 - **Management State:** Displays the monitoring state of the controller. *Active or Inactive*.
 - **Management Server Message:** Displays the management server message.
 - **N+1 State:** Displays the *N+1 State*. The possible ones are
 - Not Configured
 - Master
 - Active Slave
 - Active
 - Unknown.
 - **Uptime:** Displays the Controller's current uptime in days, hours, minutes, and seconds.

Import Controllers to Inventory

You can add Controllers into Inventory by importing files (*.CSV).

Click **Download Default Template** to download the default template to add a Controller.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP Po
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
23												
24												
25												
26												
27												
28												
29												
30												
31												
32												
33												

Edit and save the template. The HostName, User Name, and Password are mandatory fields. Modifying the Controller ID will not take effect as the reset of the fields are identified with the Controller ID.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP I
2		10.34.115.23			admin	admin						
3												
4												

Click **Import** and browse to the saved *.csv template file. Click **Upload**.

In case of errors, view the import logs using the **View Latest Import Log** option for error details.

View Import Log	
HOSTNAME/IP ADDRESS	ERROR
<input type="text"/>	
10.34.159.215	SSH Port can be 22 or between 1024 to 65535
1 - 1 of 1	

Export Controllers from Inventory

You to export the existing Controllers to your local drive.

Controller

REFRESH

ADD









DELETE

IMPORT

EXPORT ALL

AUTO SAVE CONFIGURATION

DOWNLOAD DEFAULT TEMPLATE

ID	HOSTNAME/IP ADDRESS	IP ADDRESS	NODE NAME	SOFTWARE VERSION	CONTROLLER MODEL	AVAILABILITY STATE	MANAGEMENT STATE	CONTROLLER GROUP	AUTO SAVE CONFIG	ACTION
44	10.34.133.230	10.34.133.230	meg-3200	8.3-1GAbuild-0	MC3200	Online	Active	default	Off	 
38	10.34.135.220	10.34.135.220	uma	8.3-0GAbuild-100	MC1550	Online	Active	default	Off	 
39	10.34.143.16	10.34.143.16	default	6.1-3-6	MC3200-VE	Online	Active	default	Off	 
43	10.34.143.14	10.34.143.14	default	5.3-164	MC3200-VE	Online	Inactive	default	Off	 

< > 1 - 4 of 4 > >

View Latest Import Log

Note:

The **Export All** option does not export the Controller password.

The exported Controller.csv can be edited and imported

	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP Port
2	7	10.33.115.28		22	admin		default	Use Default	0.0.0.0	On	Managed	443
3	4	10.34.133.230		22	admin		default	Use Default	0.0.0.0	Off	Managed	443
4	3	10.33.115.23		22	admin		default	Use Default	0.0.0.0	Off	Managed	443
5												

Auto Save Controller Configuration

To automatically save Controller configuration updates, select one or multiple Controllers and set the **Auto Save Configuration** to **On**.

REFRESH

ADD









DELETE

IMPORT

EXPORT ALL

AUTO SAVE CONFIGURATION

DOWNLOAD DEFAULT TEMPLATE

ID	HOSTNAME/IP ADDRESS	IP ADDRESS	NODE NAME	AUTO SAVE CONFIG	CONTROLLER MODEL	AVAILABILITY STATE	MANAGEMENT STATE	CONTROLLER GROUP	AUTO SAVE CONFIG	ACTION	
8	10.34.133.230	10.34.133.230	default	ON	8.3-1GAbuild-0	MC3200	Online	Active	default	Off	 
7	10.34.135.220	10.34.135.220	default	OFF	8.3-0GAbuild-100	MC1550	Online	Active	default	Off	 
9	10.33.115.28	10.33.115.28	default		8.3-2build-34	MC1550	Online	Active	default	Off	 
6	10.34.140.140	10.34.140.140	default		8.2-7MR-1	MC4200-VE	Online	Active	default	Off	 

< > 1 - 4 of 4 > >

View Latest Import Log

To disable automatically saving the Controller configuration, set the **Auto Save Configuration** to **OFF**.

The **Auto Save Config** column is updated.

Access Points

1. Navigate to *Inventory > Devices > Controllers*.
2. In the *Controllers* screen, select a controller by clicking the check box and select the *Edit* option.
3. Select the *Access Points* tab. The *Access Points* screen displays a list of APs mapped to the selected controller.
4. In the *Access Points* screen, select a access point by clicking the check box and select the *View Details* option.

5. In the *Access Points - Details* screen you can view the following fields:

Field	Description
Controller ID	Displays the controller Id to which the AP is mapped.
AP ID	Displays the AP ID.
Serial Number	Displays the serial number of AP, which is always the Ethernet MAC address.
Uptime	Displays the uptime of AP.
Location	Displays the location of the AP.
Building	Displays the building name where the AP is located in.
Floor	Displays the floor name where the AP is located.
Contact	Displays the person or organization responsible for the access point.
Discovery Protocol	Displays the discovery protocol.
Connectivity Layer	Displays the Network layer through which the access point is connected to the controller: <ul style="list-style-type: none"> • L2: Access point is in the same subnet as controller. • L3: Access point is in a different subnet from controller and connected to controller through a router.
Management Administrative State	Displays the management administrative state if managed, deleted, maintenance, or unlicensed.
Operational State	Displays the operational state is enabled or disabled.
Availability Status	Displays if the controller is reachable or not from FortiWLM. <ul style="list-style-type: none"> • Online indicates reachable • Offline indicates not-reachable.
AP Model	Displays the AP model number.
Runtime Image Version	Displays the version of the operating system image on the access point. This version should always match the software version for the controller.
Boot Image Version	Displays the version of the ROM boot image on the access point.
FPGA Version	Displays the version of the FPGA chip on the access point (not supported for AP150, RS4000, OAP180, or AP300).

Field	Description
AP Role	<p>Displays the role which the AP plays in the WLAN. The following are the AP role types:</p> <ul style="list-style-type: none"> • Access: Access point is operating as a standard, wired AP. • Wireless: Access Point is part of the Enterprise Mesh configuration, providing wireless access services to 802.11/b/g clients and backhaul services on the 802.11/a link. • Gateway: Access point is part of the Enterprise Mesh configuration, providing the link between the wired and wireless service.
Parent MAC Address	Specifies the MAC address of the parent AP when Enterprise Mesh is configured.

6. Select *Back* to go back to the *Access Points* screen.

Access Points Inventory

All FortiWLC run *System Director*, (the Fortinet operating system) that centrally manages and monitors access points (APs). System Director provides a centralized management system accessed from either the web UI or a *Command Line Interface* (CLI) for monitoring, configuration, and troubleshooting the system. The *FortiWLM* manages multiple *FortiWLC*. One of the major features of this product is the ability to create a global from *FortiWLM* and download it to one or more managed controllers. These global s are owned by E(z)RF server and cannot be altered by the controllers using them. The *FortiWLM* supports controllers running on a *Fortinet Services Appliance* hardware device or on a virtualized environment based on VMware.

How AP Discovery Works

There are three types of access point discovery:

- Layer 2 only—Access point is in same subnet as controller.
- Layer 2 preferred—Access point sends broadcasts to find the controller by trying Layer 2 discovery first. If the access point gets no response, it tries Layer 3 discovery.
- Layer 3 preferred—Access point send broadcasts to find the controller by trying Layer 3 discovery first. If the access point gets no response, it tries Layer 2 discovery.

For Layer 2 and Layer 3 discovery, the access point cycles between Layer 2 and Layer 3 until it finds the controller. The access point waits 16 seconds before cycling between Layer 2 and Layer 3.

An access point obtains its own IP address from DHCP (the default method), or you can assign a static IP address. After the access point has an IP address, it must find the controller. By default, when using Layer 3 discovery, the access point obtains the controller's IP address by using DNS and querying for hostname "*wlan-controller*." This presumes the DNS server knows the domain name where the controller is located. The domain name can be entered via the AP configuration or it can be obtained from the DHCP server, but without it, a Layer 3-configured AP will fail to find a controller. Alternately, you can configure the AP to point directly to the controller's IP address (if the controller has a static IP configuration).

Once the access point obtains the controller IP address, it sends broadcast messages using UDP port 9393. After the controller acknowledges the messages, a link is formed between the AP and the controller.

Access Points tab

1. Navigate to *Inventory > Devices > Access Points*. The *Access Points* screen provides you a list of online and offline APs that are managed by the controllers.
2. You can perform the following actions on the *Access Points* screen.
 - **View:**
 - Select the *AP Name* hyper link.
 - The *Access Points* details, *AP Group Membership*, *Wireless Interface*, and *Connectivity* details of the selected AP is displayed.
 - **Filter:** Select the *Filter* option. The *Location Filter* allows you to filter the APs by the *Campus*, *Building*, and *Floor*.
 - **Delete APs:** The Offline APs can be deleted from the NM AP inventory. The selected APs can be deleted from inventory and geographical map assignment and clears any outstanding alarms related to the AP. It also releases respective licenses, if any. The delete option, does not delete the historical statistics collected on the serve.
 - **Edit:** You will be able to edit the *Administrative State* from *managed* to *maintenance*.
 - **Show AP Dashboard:** Select the *Show AP Dashboard* icon to view the details of the selected AP. The AP Dashboard screen displays an in-depth information about the AP activity. It provides you a graphical representation of the *Throughput*, *Station Count*, *Noise Level*, *Loss%*, and *Channel Utilization%* of each radio on AP connected to the controller which is managed by FortiWLM.
 - **Show AP Location:** Select the *Show AP Location* icon, to view the location of the selected AP in the enterprise, campus, building, and floor.

Figure 76 on page 213 illustrates the *Access Points* screen.

Figure 76: Access Points

Access Points

AP Replacement

1 - 8 of 8

FILTER

<input type="checkbox"/>	AP NAME	IP ADDRESS	SERIAL NUMBER	AP MODEL	DISCOVERY PROTOCOL	RUNTIME IMAGE VERSION	AVAILABILITY STATUS	UPTIME	CONTROLLER	ACTIONS
<input type="checkbox"/>	AP-1	172.19.32.192	00:0c:e6:0c:f0:8f	AP1010	L3 preferred	6.0-8-0	Online	02d:12h:55m:38s	172.19.43.251	
<input type="checkbox"/>	AP-1	172.19.32.43	00:0c:e6:0d:f0:d7	AP332e	L3 preferred	5.3-149-1	Online	03d:08h:01m:05s	172.19.43.227	
<input type="checkbox"/>	AP-2	172.19.32.160	00:0c:e6:0d:ef:1f	AP332i	L3 preferred	5.3-149-1	Online	03d:08h:01m:05s	172.19.43.227	
<input type="checkbox"/>	AP-4	172.19.32.32	00:0c:e6:0c:f0:34	AP1010	L3 preferred	6.0-8-0	Online	02d:09h:11m:40s	172.19.43.251	
<input type="checkbox"/>	AP-8	172.19.32.53	00:0c:e6:0c:f0:50	AP1010	L3 preferred	6.0-8-0	Online	02d:12h:55m:42s	172.19.43.251	
<input type="checkbox"/>	AP-9	172.19.32.74	00:0c:e6:0c:ef:7a	AP1010	L3 preferred	6.0-8-0	Online	02d:12h:55m:40s	172.19.43.251	

AP Replacement

The *AP Replacement* allows you to replace a single AP or multiple APs from *NM*. The replacement of APs may be due to RMA or network upgrades such as replacement of all AP150's with AP 300's. The APs, when replaced on a controller is updated on *NM* also.



During the controller reboot, the AP replacement entries pushed from *NM* are preserved only if running-config is saved to startup-config.

Figure 77 on page 214 illustrates the *AP Replacement* screen.

The AP replacement screen is divided into the following sections:

- Pending AP Replacement (See [“Pending AP Replacement” on page 214](#))
- AP replacement History (See [“AP Replacement History” on page 215](#))

Figure 77: AP Replacement

Access Points

AP Replacement

AP Replacement History

Pending AP Replacement

+

DATE/TIME	CONTROLLER	AP MACADDRESS	NEW AP MACADDRESS	STATUS	DESCRIPTION

UPLOAD CSV

APPLY

DELETE

Back to top

AP Replacement History

1 - 3 of 3

DATE/TIME	CONTROLLER	AP MACADDRESS	NEW AP MACADDRESS	STATUS	DESCRIPTION
11/22/2013 13:57:53	172.19.43.227	00:0c:e6:0d:f0:d7	00:0c:e6:0c:f0:8f	Failed	Operation failed. New AP already exists, AP replacement cannot be performed as AP ID and Controller ID of APs to be swapped are not same.
11/22/2013 14:08:29	172.19.43.251	00:0c:e6:0c:f0:34	00:0c:e6:0c:f0:8f	Success	AP replacement performed Successfully.
11/22/2013 14:45:35	172.19.43.251	00:0c:e6:0c:ef:7a	00:0c:e6:0c:f0:50	Success	AP replacement performed Successfully.

DELETE

Pending AP Replacement

The following actions can be performed on the Pending AP Replacement (See [Figure 77 on page 214](#)) section:

- **View the list of replaced APs:** You can view a list of the replaced APs from the *AP Replacement History* option.
- **Add option for AP replacement:**
 - The *Add* icon allows you to select APs for replacement. An AP pair is replaced only if you possess access to the selected AP to be replaced.
 - A validation of the AP pair's MAC addresses is performed in the AP Replacement table, before the replacement.
 - For a new AP on *NM*, the *controller Id* and the *APID* is verified against the old AP.
 - The new AP is pushed to the controller for AP replacement. If the AP replacement is unsuccessful on the controller, the entry is deleted on the *NM* also. Upon successful completion, you are notified with the successful operation message.
 - The AP Replacement view will provide you a list the newly added AP pairs and the Replacement status is displayed as *Replaced*.
 - If the Replacement is awaiting physical replacement of the equipment, the status is displayed as *Replacement Pending*. The status is modified to *Replaced* once the replaced AP is online on the *NM*.

- **Upload a list of APs to be replaced through a CSV report:** Multiple APs are replaced by selecting this option. A list of AP names are separated by coma separated values and saved in the CSV format on the local hard drive. The CSV file is uploaded to the *NM* server and the back end script validates the entries and creates entries in AP Replacement table. The CSV report consists of the *AP MAC-Address* and the *New AP MAC-Address*.
- **Delete an AP pair from the list:** The deletion of the AP pair on the AP Replacement table, not only deletes the AP pair on the *NM* but also deletes the AP pair on the controller, if the affected controller appears online. The AP Replacement delete operation fails, if the Status of the selected AP Replacement entry is *Pending* and the Status of the Controller is *Offline*. The AP Replacement Status is displayed as *Delete Failed*.

AP Replacement History

The *AP Replacement History* table provides you a complete history of the APs replaced with the details like *Date/Time*, *Controller*, *AP MAC Address*, *New AP MAC Address*, *Status*, and *Description*. Select an AP and select *Delete* on the *AP Replacement History* table, to delete the history of the AP. Only three months old data is deleted from the AP Replacement History table. See [Figure 77 on page 214](#).

Switches

The *Switches* are third party devices that use SNMP credentials for detecting the *Wired Rogues*. The switches screen displays a list of switches managed by the *FortiWLM*.

1. Select *Inventory > Devices > Switches*.
2. The *Switches* screen displays the details of the switches such as *Host Name / IP Address*, *Model*, *Description*, and *Status*. See [Figure 78 on page 216](#).

Figure 78: Switches - Add

Switches - Add

HOSTNAME/IP Address	<input type="text" value="Test"/>	[1-255] chars., Required
SNMP Version	<input type="text" value="SNMP Version V3"/>	
Username	<input type="text"/>	[1 - 255] chars., Required
Authentication protocol	<input type="text" value="No Authentication"/>	
Authentication String	<input type="text"/>	[1 - 255] chars., Required
Privacy protocol	<input type="text" value="No Privacy"/>	
Privacy String	<input type="text"/>	[1 - 255] chars., Required

3. The *Add* option allows you to include a switch. The details such as *Host Name / IP Address*, *SNMP Version*, and *SNMP Community String* is provided.
4. The *Edit* option allows you to *Edit* the existing switch details.

Groups

The *Controllers* and *APs* are grouped for monitoring and configuration purpose. The groups are assigned to a user group. The following screens in the Inventory allows you to group controllers and APs:

- “*Controller Group Inventory*” on page 216
- “*AP Group Inventory*” on page 219

Controller Group Inventory

The controllers can be grouped and assigned to a user group. Each controller can belong to one controller group only; if a controller is added to a second group, it is automatically removed from the previous group. However, controller groups can be assigned to multiple user groups.

Users can also be grouped and assigned group privileges from the web UI of *FortiWLM*. Only users with administration capability can modify a user group; *Administrators* can assign one or all permissions to their own user group.

A Controller group can be created using a set of controllers belonging to a particular user or user group. This allows the users belonging to the user group to have access to those controllers. For example, the controller drop-down list on the various dashboards display the control-

lers assigned to the current user group. The user must have inventory access permissions, to add, delete, view, or move controllers from one controller group to other.

Both controller groups and user groups are included in a backup.

If you do not set up controller groups, all controllers remain assigned to the controller group named *Default*. The controller group named *Default* can always be changed by the two permanent user groups named *Superuser* and *Default* user. The two permanent user groups, *Default* and *Superuser*, cannot be deleted.

Add a Controller Group

Only users having *Inventory* access permissions will be able to add a group, delete a group or move controllers from one group to the other. If you add a controller that already belongs to a group, the controller is removed from the old group and added to the new one. To create a controller group and add controllers to it, follow these steps:

1. Create the controller group by clicking *Inventory > Devices > Controller Groups > Add*.
2. In the *Controller Group - Add* screen provide a *Group Name* and optional *Description*. This is all that is required to create the group. You can click *Save* now if you wish. See [Figure 79 on page 217](#) illustrates the *Controller Groups - Add* screen.

Figure 79: *Controller Groups - Add*

Group Name

[1-255] chars., **Required**

Description

[0-128] chars.

Members

[Add](#) [Delete](#)

<input type="checkbox"/>	Host Name	Description	Controller Model
<input type="checkbox"/>	172.19.43.227	controller	MC1550
<input type="checkbox"/>	172.19.43.229	controller	MC1550

Note: Controllers belong to only one group. Adding a controller to a group, moves the controller to the selected group.

3. Optionally, add controllers to the group by clicking *Add*. A list of controllers present in the Inventory is displayed. Select one of the listed controllers - all of them are working with *FortiWLM* and click *OK*. The new controller is added to the list of controller groups.
4. Each *Controller Group* is assigned to a *Group Id*. The *Default* group comprises of the Group Id as 1.

5. To use the controller group, associate it with one or more user groups. To do this, see either *Add a User Group* or *Modify a User Group*.

Modify a Controller Group

Only users having *Inventory* access permissions will be able to add a group, delete a group or move controllers from one group to the other. (See *“User Group Access Capabilities” on page 295* for details on assigning permissions for Inventory access.) To modify a controller group, follow these steps:

1. Navigate to *Inventory > Devices > Controller Groups > select a controller group > Edit*.
2. In the *Controller Groups - Update* screen, modify the *Group Name*, *Description*, and add or delete controllers if required. If you delete controllers from a group, they are automatically reassigned to the group *Default*. *Figure 80 on page 218* illustrates the *Controller Groups - Update* screen.

Figure 80: Controller Groups - Update

Controller Groups - Update

Group Id

3

Group Name

[1-255] chars., **Required**

Description

[0-128] chars.

Last Updated

11/25/2013 06:28:12

Members

[Add](#) [Delete](#)

<input type="checkbox"/>	Host Name	Description ↕	Controller Model
<input type="checkbox"/>	172.19.43.229	controller	MC1550
<input type="checkbox"/>	172.19.43.227	controller	MC1550

Note: Controllers belong to only one group. Adding a controller to a group, moves the controller to the selected group.

Delete a Controller Group

Only users having *Inventory* access permissions will be able to add a group, delete a group or move controllers from one group to the other. (See *“User Group Access Capabilities” on page 295* for details on assigning permissions for Inventory access.) The *Controller Groups* which consists of controllers within the group cannot be deleted. Remove all controllers from a group before deleting the groups.

To delete an empty controller group, follow these steps:

1. Navigate to *Inventory > Devices > Controller Groups*.
2. In the *Controller Groups* screen, select one or more check boxes corresponding to controller groups.
3. Click *Delete*. The selected controller is deleted from the *Controller Groups* screen.

AP Group Inventory

The *AP Groups* screen displays a list of AP Groups. An *AP Group* is a hierarchical representation of all the APs assigned to the selected group to which the user has scope. The AP Groups screen allows you to create an AP group and assign APs to the group created. The APs within the selected AP Group is used to create *AP Group Dashboard* data, which is generated every 5 minutes on the server. See [“AP Group Summary” on page 42](#).

The AP Groups are classified into the following types:

- **Monitoring and Service Configuration:** The *Monitoring and Service Configuration* group is identical to that of an AP Group to which the Service Profile is applied.
- **Device Administration:** The *Device Administration* group, a specialized AP Group which applied to the device settings such as *Radio* and *Connectivity Profiles* (See [“Radio Profile” on page 151](#) and [“Connectivity Profile” on page 151](#).) This group has a restriction that an AP can belong to only one *Device Administration* group. This restriction prevents multiple device configurations getting applied from different groups.

An AP group may belong to multiple AP Groups. It can be created by using APs on the same controller or by using APs from multiple controllers. It may consist of APs of different hardware model, or APs from controllers running different system director versions.

The *AP Groups* screen displays the following sections: (See [Figure 81 on page 220](#) illustrates the *AP Groups* screen.)

- **Hierarchical view of AP Groups:** Displays the *AP Groups*, *Subgroups* and *APs* of the Controller as a hierarchy. Each AP Group displays several subgroups. Select icon to view the AP Groups, Subgroups and APs of the Controller.
- **Summary:** Provides the details like *AP Name*, *Description*, *Last Updated Time*, *Owner*, and *Usage details*.
- **Member Sub Groups:** Provides the list of *Sub Groups* under the selected *AP Group*. A sub group can be added or deleted by selecting the respective options.
- **Member APs:** Provides a list of APs, under each *Sub Group* of the selected AP Group.

Figure 81: AP Groups

AP Groups

Enterprise

Meru

Groundfloor

Salarpuria-groundflr

Salarpuria-firstflr

Salarpuria-firstflr-device

Salarpuria-groundflr-device

test

Demo-Group

Summary

Name	Salarpuria-groundflr	Description	Salarpuria-groundflr	Last Updated Time	09 Aug 2012 14:58:16
Owner	admin	Usage	Monitoring and Service Configuration		

EDIT

Member Sub Groups

+
NAME DESCRIPTION

DELETE

Member APs

<< 1 - 1 of 1 >>

+
CONTROLLER AP NAME IP ADDRESS MAC ADDRESS MODEL SOFTWARE VERSION LOCATION

<input type="checkbox"/>	172.16.16.16	AP-9	0.0.0.0	00:0c:e6:07:d6:3e	PSM3x	5.3-132	
--------------------------	--------------	------	---------	-------------------	-------	---------	--

DELETE

Dynamic AP group

By default, APs connected to a controllers are added into an AP group. This is done based on the controllers IP address. This is also called the default dynamic AP group. The default group cannot be modified or deleted and APs in that group cannot be removed. Dynamic groups are available only for service and monitoring and cannot be used for device administration.

Add

Name * [1-64] chars.

Description [0-255] chars.

Group ☐ Static ☒ **Dynamic**

Usage ☒ Monitoring and Service Configuration ☐ Device Administration

Rule Condition ☒ Match All Rules ☐ Match Atleast One Rule

	Rules	Operator	Value
<input type="checkbox"/>	Controller ▼	Equals ▼	Please Select Value ▼

Note:

- An AP can exist in more than one dynamic groups.
- A dynamic group can be created inside a static group.
- Any modification to the rule will affect the APs in the group.

To create custom dynamic groups, you can set rules using AND or OR conditions. The APs can be set to a dynamic group if all rules match or if at least one rules matches. The following filter are available to create rules:

- Controller IP address
- Location
- Building
- Floor
- Discovery Type (L2 or L3)
- AP Model
- Software Version

- AP Description
- Parent MAC Address
- Indoor / Outdoor APs

Current Upgrades

The *Current Upgrades* screen provides you the details of the controller upgrades that are in progress and in completed state during the last one hour. Individual *Controllers* or *Nplus1* controllers are upgraded here. It allows you to perform controller upgrade and keep track of the controllers that are in the process of getting upgraded.

To apply a *System Director* image to controllers, follow these steps:

1. Navigate to *Inventory > Software Upgrades > Current Upgrades*. [Figure 83 on page 224](#) illustrates the *Current Upgrades* screen.

Figure 83: Current Upgrades

Current Upgrades

Auto Refresh : 50 Secs

<input type="checkbox"/>	HOSTNAME	IMAGE NAME	UPGRADE GROUP	UPGRADE TYPE	PHASE	STATUS	ERROR	UPGRADE DETAILS	UPGRADE PROGRESS
<input type="checkbox"/>									

Select Controllers/Nplus1 Clusters to upgrade

Image Name

Select Version

Upgrade Group

Individual Controllers

Upgrade Type

Controller

Online Controllers

CLOSE

SAVE

2. The *Current Upgrade* screen displays a list of *Master, Slave and Individual Controllers* for which the upgrade process is initiated. The following are the details:

Field	Description
Host name	Displays the <i>Host Name</i> of the controller.
Image Name	Displays the <i>Image</i> to be upgraded.
Upgrade Group	Displays the <i>Upgrade Group</i> of the controller. The two types are as follows: <ul style="list-style-type: none">• Individual controllers• Nplus1 Clusters

Field	Description
Upgrade Type	Displays the <i>Upgrade Type</i> of the controller. The two types are as follows: <ul style="list-style-type: none"> • Controller • Access Points and controller • Feature • Patch-Controller
Phase	Displays the phase of the controller.
Status	Displays the <i>status</i> of the controller. The four types are as follows: <ul style="list-style-type: none"> • In Progress - The controller is <i>In Progress</i> for up gradation. • Pending - The controller is still pending for up gradation. • Success - The controller has successfully upgraded. • Failed - The controller has failed to upgrade. In Nplus1 upgrade, <ul style="list-style-type: none"> • Success indicates a successful upgrade of the controller with the right image and start the Nplus1 server. • Failed indicates a failure in upgrade of the controller with the right image and failed to start Nplus1 server.
Error	Displays the <i>Error</i> message during the failure of the controller upgrade.
Upgrade Details	Displays the <i>Upgrade Details</i> of the slave controller. Select the <i>Detail</i> link to view the <i>Log Details</i> . The <i>Slave Log</i> file displays the information about the slave and high level information about the masters.
Upgrade Progress	Displays the cluster <i>Upgrade Progress</i> of the slave controller. The initial upgrade is progressed by the slave controller followed by the master controllers.

Select a *Slave Controller*, the respective *Master Controllers* can be viewed below the selected slave controllers.

3. You can perform the following actions on the *Current Upgrades* screen:

- Expand All
 - Select *Expand All* option.
 - You can view the complete details of the slave controllers and master controller.
- Collapse All
 - Select *Collapse All* option.
 - The details of the slave controllers and master controller is compressed.
- Add

- Select the *Add* icon. This option allows you to upgrade a controller
- In the *Select Controllers/Nplus1 Clusters to upgrade* screen you can view the following details of individual controllers and nplus1 cluster controllers.

Field	Description
Image Name	Select the <i>Image</i> to be upgraded.
Upgrade Group	<p>Select the <i>Upgrade Group</i> of the Controller. The two types are as follows:</p> <ul style="list-style-type: none"> • Individual Controllers: The <i>Individual Controllers</i> displays the list of Individual controllers listed on the <i>FortiWLM</i> server. • Nplus1 Clusters: The <i>Nplus1 Clusters</i> displays a list of <i>Slave Controllers</i> and <i>Master Controllers</i> that are located on the <i>FortiWLM</i> server. <p>Select a <i>Slave Controller</i>, the respective <i>Master Controllers</i> can be viewed below the selected <i>Slave Controllers</i>.</p>
Upgrade Type	<p>Select an <i>Upgrade Type</i> from the drop-down list as follows:</p> <ul style="list-style-type: none"> • Controller: This is equivalent to the command <i>upgrade controller</i>. It upgrades the controller. • Access Points and Controller: This is the equivalent to the command <i>upgrade system</i>. It upgrades the <i>APs</i> and <i>controller</i>.
Schedule Upgrade	You can schedule controller upgrades to happen at different times and with different images. Select Later and then use the date picker icon to select the date and time. If you select Later , you have the option to copy the image to the controller but perform the installation process at a later scheduled time.

- Click *Save* to proceed. The recently added *Select Controllers* or *Nplus1 Clusters* is displayed on the *Current Upgrades* screen.
- Delete
 - In the *Current Upgrades* screen, select one or more controllers from the drop-down list and click on *Delete*.
 - The selected controllers are deleted.
 - For *Nplus1*, the delete function, deletes the *Slave and the Master Controllers*.

The upgrade status older than one hour is available under *Inventory > Software Upgrades > Upgrade History*.

Upgrade History

You can view the complete history of *successfully* upgraded controllers and *failed* controllers.

Field	Description
Start Time	Displays the upgrade start time.
End Time	Displays the upgrade end time.
User	Displays the controller user name.
Controller	Displays the controller host name.
Previous Version	Displays the previous version of the controller before upgrade.
Next Version	Displays the next version of the controller after upgrade.
Upgrade Group	<p>Displays the upgrade group of the slave controller. The two types are as follows:</p> <ul style="list-style-type: none">• Individual Controllers: Displays a list of controllers selected for upgrade on the nms-server.• Nplus1 Clusters: Displays a list of slave controllers and master controllers that are located on the nms-server.
Upgrade Type	<p>Displays the upgrade type. The two types are as follows:</p> <ul style="list-style-type: none">• Controller: This is equivalent to the controller upgrade command. It upgrades the controller.• Access Points and Controller: This is equivalent to the command upgrade system. It upgrades the Access Points and Controller.
Phase	<p>Displays the different phases of the controller upgrade. Following are the types:</p> <ul style="list-style-type: none">• Image copy• Upgrade APs• Upgrade controller• Upgrade complete
Status	<p>Displays the status of the controller. Following are the types:</p> <ul style="list-style-type: none">• Success - The controller is successfully upgraded.• Failed - The controller has failed to upgrade.

Create an Upgrade Schedule

Select Controllers/Nplus1 Clusters to upgrade

Image Name: meru-8.0-5-0-MC1550-rpm.tar

Upgrade Group: Individual Controllers

Upgrade Type: Controller

Schedule Upgrade: ☐ Now ☒ Later 03/22/2016 17:47:00

Online Controllers

CONTROLLER NAME	DESCRIPTION	HARDWARE TYPE
172.18.215.225	controller	MC1550

Calendar: MARCH 2016

Time: 17 : 47

CANCEL SAVE

Configured Upgrade Schedules

Current Upgrades ?

CURRENT UPGRADES

< 1 - 1 of 1 >

	CONTROLLER NAME	IMAGE NAME	UPGRADE GROUP	UPGRADE TYPE	PHASE	STATUS	SCHEDULED AT
	172.18.215.225	meru-8.0-5-0-MC1550-rpm.tar	Individual Controller	Controller	Image Copy	Scheduled	22/3/2016 17:47:0

Reschedule Upgrades

To reschedule, select a controller and click the Reschedule Button.

Upgrade Limitations

When an environment has an Nplus1 cluster with two different models (example: MC4200 and MC4200V combination), these controllers are not listed while trying to upgrade them from For-tiWLM. When you select MC4200/MC4200V image in Upgrade management, it is not listed in either under cluster (since it has two different models) or under individual controllers (since it is a cluster).

6 Visualization

The *Visualization* feature is an interactive heat map that allows you to verify the coverage and performance of your WLAN APs. You can also use the maps to visually locate APs sending alarms. Use the map editor to set up your site maps.

Heat Maps

1. Navigate to *Visualization > Heat Maps*.
2. In the *Network Heat Maps* screen, select a *Location* from the menu on the left to see the corresponding map.
3. Hover the mouse pointer over the objects on the screen to see details. For example, for this throughput map, by hovering the mouse pointer on an AP icon displays the *Name*, *model*, *Mac Address*, *status of the AP* and *throughput value*. If you change the *Heat Map Type*, be sure to click *Refresh* icon.
4. In the *Network Heat Maps* screen select a floor. The following five types of heat maps can be viewed.

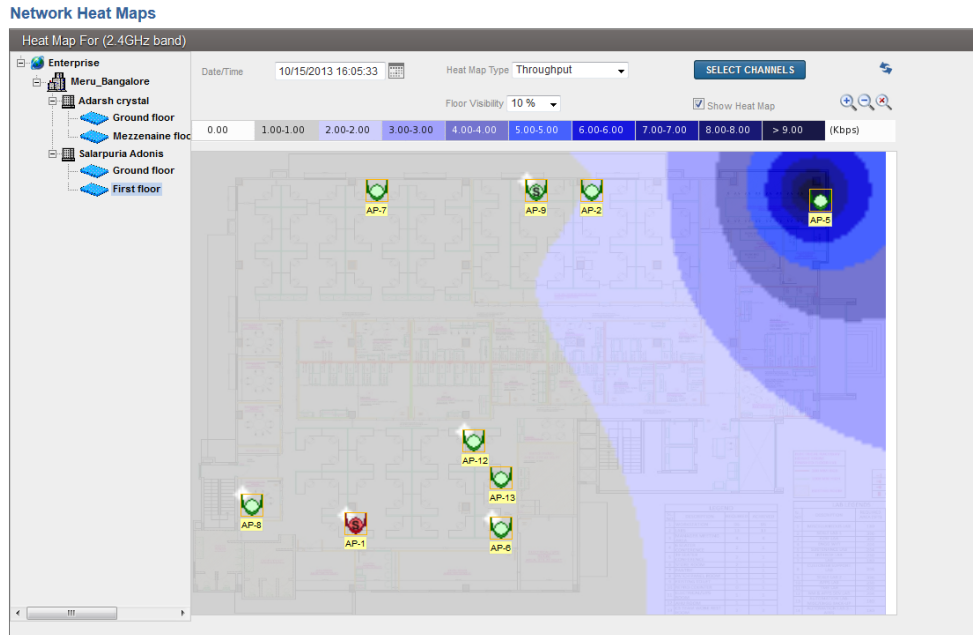
Throughput Heat Map

Throughput maps display the AP throughput over the area represented by the map. The APs on the map is differentiated by using different colors for the regions around APs corresponding to the AP throughput value. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC Address
- Status of the AP
- Throughput in Kbps.
- Right click an *AP* and select *Show Details* to view the *AP details* and *Station details*.
 - **AP details:** *AP ID, AP Name, AP MAC, AP IP Address, Controller, and Total Stations.*
 - **Station details:** *MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, and L3 State.*

- Click the MAC address to view the *Station Trend Dashboard*. [Figure 85 on page 232](#) illustrates the *Throughput Heat Map*.

Figure 85: Throughput Heat Map



The filtering option comprises of *All*, *2.4 GHz [default]*, *5 GHz* and *selected* channels within the two bands.

Loss Heat Map

Loss maps show AP loss over the area represented by the map. The *Loss* maps differentiate APs on the map by using different colors for the regions around APs corresponding to the AP Loss% value. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC
- Status
- Loss(%)
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*.
 - **AP details:** *AP ID, AP Name, AP MAC, AP IP Address, Controller, and Total Stations*

- **Station details:** MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, and L3 State.
- Click the MAC address to view the *Station Trend Dashboard*. [Figure 86 on page 233](#) illustrates the *Loss Heat Map*.

Figure 86: Loss Heat Map



The filtering option comprises of *All*, *2.4 GHz [default]*, *5 GHz* and *selected* channels within the two bands.

Channel Utilization Heat Map

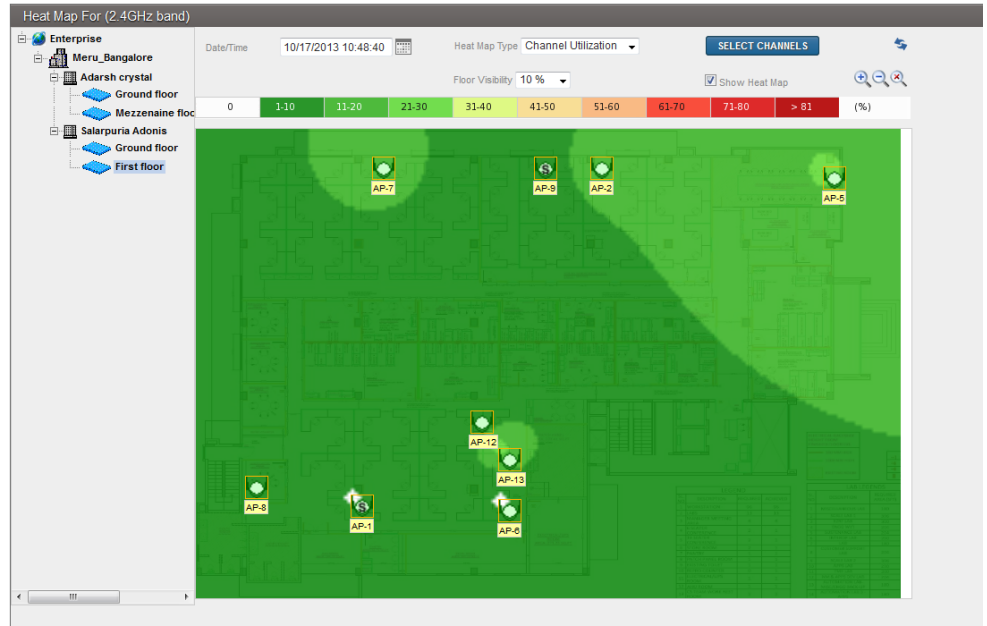
The *Channel Utilization* maps differentiate APs on the map by using different colors for the regions around APs corresponding to the AP channel utilization value. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC Address
- Status
- Channel Utilization (%)
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*:

- **AP details:** AP ID, AP Name, AP MAC, AP IP Address, Controller, and Total Stations.
- **Station details:** MAC Address, IP address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, and L3 State.
- Click the MAC address to view the Station Trend Dashboard. [Figure 87 on page 234](#) illustrates the Channel Utilization Heat Map.

Figure 87: Channel Utilization Heat Map

Network Heat Maps



The filtering option comprises of *All*, *2.4 GHz [default]*, *5 GHz* and *selected* channels within the two bands.

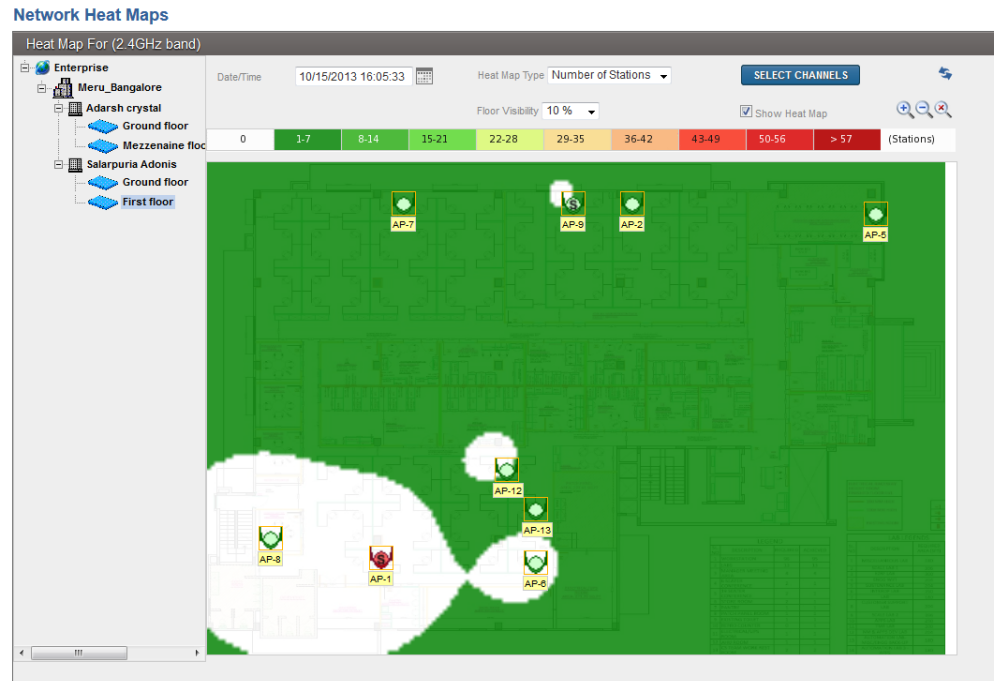
Number of Stations Heat Map

The Number of Stations Heat Map, represents the low signals over the area represented by the map. The Number of Stations maps differentiate APs on the map by using different colors for the regions around APs corresponding to the number of stations per AP. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC Address
- Status of the AP
- Number of Stations

- Right click an AP and select *Show Details* to view the *AP details* and *Station details*:
 - **AP details:** *AP ID, AP Name, AP MAC, AP IP Address, Controller ID, and Total Stations.*
 - **Station details:** *MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, and L3 State.*
- Click the MAC address to view the *Station Trend Dashboard*. [Figure 88 on page 235](#) illustrates the *Number of Stations Heat Map*.

Figure 88: Number of Stations Heat Map

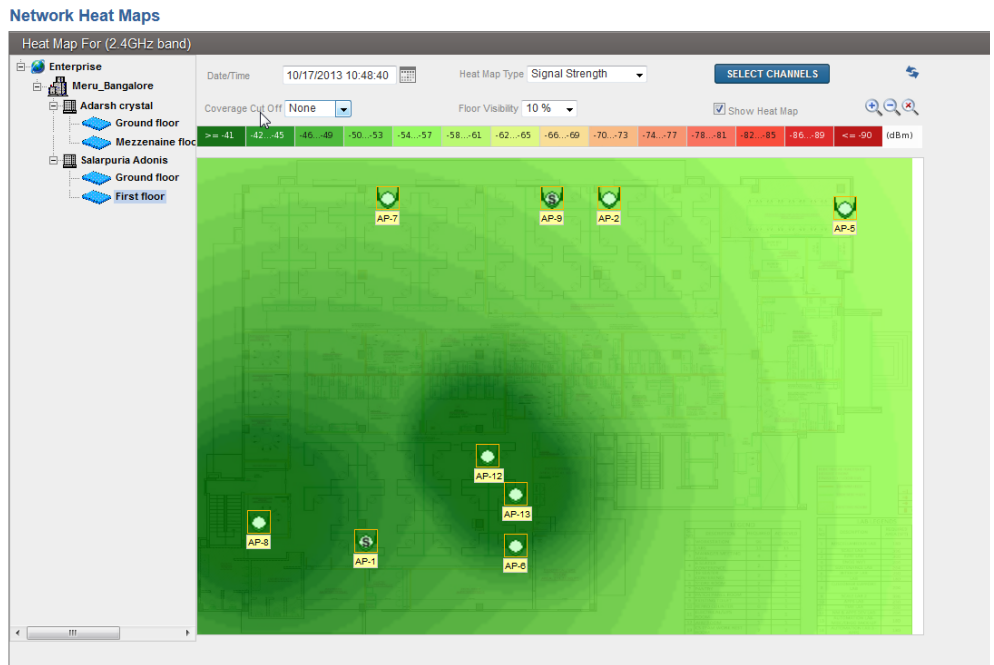


The filtering option comprises of *All, 2.4 GHz [default], 5 GHz* and *selected channels* within the two bands.

Signal Strength Heat Map

Signal strength heat map provides a distribution of signal quality over the floor map. The signal strength is represented in dBm and is divided into color buckets. The *Signal Strength* maps display the availability of signal over the area represented by the map. Select different cut-off values to view the signal coverage.

Figure 89: Signal Strength Heat Map



The signal strength heat map allows you to view the signals of all the APs on the floor. Due to this, the FortiWLM displays heat map for all APs irrespective of whether the logged in user has scope for those APs or not. This enables you to capture accurate signal value for all APs located on the floor

Select a location from the menu on the left to see the corresponding map. Move your mouse over the AP icon to display the following:

- AP Name
- AP Model
- AP MAC
- Status of the AP
- Signal Strength
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*:
 - **AP details:** AP ID, AP Name, AP MAC, AP IP Address, Controller ID, and Total Stations.
 - **Station details:** MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, and L3 State.

- Click the MAC address to view the *Station Trend Dashboard*. [Figure 89 on page 236](#) illustrates the *Signal Strength Heat Map*.

The filtering option comprises of *All*, *2.4 Hz [default]*, *5 GHz* and *selected* channels within the two bands.

With signal strength heat map having smooth transition in colors, the color at a given point may not exactly match with the bucket colors. For such cases, it should be interpreted as a value that is greater/lower than the nearest bucket color.

- Coverage Cut Off:** Coverage cutoff [default being none] can be used to see the signal coverage region within the cutoff value specified. The cutoff range is from -42dBm to -90dBm.

In order to view the signal strength heat map of a floor, follow the steps:

- Ensure the APs are placed accurately through the map management feature.
- Click on the *Heat maps -> Floor*, select the RF band of choice, or the relevant channel.
- Choose a cutoff that is of interest.
- Click on *Refresh* icon.

Map Management

You can create maps to track your APs visually. Maps must accurately represent the physical layout of the site and be as close to scale as possible. We suggest using a separate map for each floor in multi-level buildings and images based on accurate architectural drawings. Crop the map of each floor to remove any extra space and save it as a PNG, JPEG, BMP, or GIF file, no larger than 2MB adding the map to NM. ([Figure 90 on page 237](#) illustrates the *Map Management* screen)

Figure 90: Map Management

Map Management

Enterprise

Meru_Bangalore

Adarsh crystal

Ground floor

Mezzenaine floor

Salarpuria Adonis

Ground floor

First floor

Summary

Name

Enterprise

(1 - 50 chars max)

Description

Top of the hierarchy

(0 - 250 chars max)

Campus Details

CAMPUS

(1 - 50 CHARS)

DESCRIPTION

(0 - 250 CHARS)

SORT ORDER

☐ Meru_Bangalore

Meru Bangalore for monitoring first set of APs

0

ADD

DELETE

There are multiple tasks required to set up a working map:

- Import a graphic map of the floor - [“Import a Map Image” on page 238](#)
- Add a new campus to FortiWLM -[“Add a Campus, Building, and Floor to the Map” on page 238](#)

- Add a building
- Add a floor
- Place AP icons on the map to depict the WLAN network topology. *“Add APs, Floor APs and Landmarks to Maps” on page 239*
- View the map - *“Viewing Maps” on page 239*

Import a Map Image

Complete the following steps to import a topology map:

1. If the Map Management screen is not displayed, click *Visualization > Map Management*.
2. Select a floor.
3. Click *Change Image* in the Image Map section.
4. Select *Image Type* as *Floor* and *Operation* as *Upload*. Select the *Image File* by using the browse tab and click on Upload.

Next, add controllers and APs to the map.

Add a Campus, Building, and Floor to the Map

Create a new location (campus, building, floor) in the enterprise by following these steps:

1. Click *Visualization > Map Management*. All current maps are displayed on the *Map Management* page.
2. A new campus can only be added to the top level, *Enterprise*, which is the default. In the *Campus Details* section, click *Add*.
3. Provide a *name*, *description*, and *sort order* for the *campus*.
4. Click *Save Changes*.
5. In the left pane, double click the name of the new campus you just created.
6. Select the *Buildings* icon. In the *Building Details* pop-up, click *Add*.
7. Provide a *name*, *description* and *sort order* for the building.
8. Click *Save Changes*.
9. In the left pane, double click the name of the new building you just created.
10. In the *Floor Details* section, click *Add*.
11. Provide a *floor name*, *length*, *width*, *metric*, and *sort order* for the floor.
12. Click *Save Changes*.

Next, import a map image (see below).

Add APs, Floor APs and Landmarks to Maps

Once a map image has been imported, add the APs to create the network map of your site. The icons should be placed on the map as close as possible to the actual physical location of the APs.

To add detail to a map, follow these steps:

1. If the *Map Management* screen is not displayed, click *Visualization > Map Management*.
2. Select a floor by its heading it in the left column.
3. You should see a map of the floor. If the floor does not yet have a corresponding map, complete the steps to *"Import a Map Image"* on **page 238**.
4. Optionally, alter the map using the options *Show Map* and *Show Scale* in the *Image Map* section.
5. Click *Add APs*, on the *AP selection* pop-up, select the APs to add from the drop-down list, then click *Save*. The selected AP appears on the map; drag it into position.
6. Add landmarks to the map by clicking *Landmarks > Add*.
7. Click *Save Changes*.

Viewing Maps

You can simply view the placement of APs on a map or you can view the *Heat Maps* using the following five attributes of those APs:

- Throughput
- Loss
- Channel Utilization
- Number of Stations
- Signal Strength

Heat map coloring depends on the distance between APs and selected attribute (throughput, loss, channel utilization, or stations) for all the APs on the floor. If there's only one AP on the floor, the entire floor will show the same coverage. View maps by following these steps:

1. Click *Visualization > Heat Maps*.
2. Select a *floor*. The map displays.
3. Optionally, alter the map using the options *Floor Visibility* or *Show Heat Map*.
4. Limit the map by clicking *Select Channels*, selecting channels, and then clicking *Save Changes*.
5. After any changes, click on *Refresh* icon.

7 Reporting and Notification in FortiWLM

Defining and Running Reports in FortiWLM

FortiWLM provides standard report types that assist you to generate, schedule and view reports. You can create and customize report types and save them as templates for future generation. Reports allow you to perform network analysis, user configuration, device optimization, and network monitoring on multiple levels. These reports provide an interface for multiple configurations, allowing you to act upon information in the reports. It also helps you to proactively identify network issues such as loss, Signal-to-Noise Ratio (SNR), station overcrowding, alarms and so on, occurred in the system.

Create Reports

FortiWLM allows you to define new reports and generate one-time reports. Perform these steps to create and run custom reports:

1. Click *Reports & Notify > Reports > Create Reports*. The *Create Reports* screen with the following sections is displayed: See [Figure 91 on page 242](#).
 - Basic Information - See [“Basic Information” on page 243](#)
 - Scope - See [“View Reports” on page 269](#)
 - Reporting Interval - See [“Reporting Interval” on page 247](#)
 - Recurrence - See [“Recurrence” on page 248](#)
 - Report Generation Options - See [“Report Generation Options” on page 248](#)

Figure 91: *Create Reports*

Create Reports

Create Reports

Basic Information

Category

Station Reports

Report Type

Station RF and Channel Dist

Sample Reports

Name

Test

Report Title

Testing

Scope

Device Selection

Default

Controllers

Controller Groups

AP

AP Groups

Station Groups

172.16.16.16

Select

Remove

Service (SSID) Selection

Select

Recurrence

One Time

Schedule

Time

12 AM

Daily

Weekly

Monthly

Every

Monday

Every

Day of Month

Reporting Interval

Last one day

Last one week

Last one month

Interval

From:

To:

Report Generation Options

File Format

HTML

PDF

Email To:

Customize

242

Defining and Running Reports in FortiWLM

Basic Information

The *Basic Information* section of the *Create Reports* screen allows you to choose a *Category of report*, *Report Type*, provide a *Name* and *Report Title*.

Figure 91 on page 242 illustrates the *Basic Information* of the *Create Reports* screen.

The supported category of reports and its report types are as follows:

TABLE 1: *Supported Report Types*

Category	Report Type	Description
Station Reports See <i>“Scope” on page 245</i>	Station RF and Channel Distribution See <i>“Station RF and Channel Distribution” on page 249</i>	Provides the station RF and channel distribution based on the OUI (Organizationally Unique Identifier). A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz and 5GHz bands and station density on each channel over time is displayed.
	Station Session Details See <i>“Station Session Details” on page 250</i>	Provides the average station session trend details. A graphical summary of the station session trend details of throughput, loss, airtime utilization and noise for a connected station is displayed.
	Top Stations See <i>“Top Stations” on page 252</i>	Lists the top interfering stations based on the throughput and airtime utilization. This report type generates the top N stations based on the number of bytes transferred and received and total Rx/Tx.
	Unique Stations See <i>“Unique Stations” on page 253</i>	Provides the unique station details based on all stations connected to a network within the reporting interval. A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz and 5GHz bands, stations distributed by OUI, stations distributed by device type, and stations distributed by OS type is displayed.

TABLE 1: Supported Report Types

Category	Report Type	Description
AP Reports	Rogue Details See <i>“Rogue Details” on page 255</i>	Summarizes individual rogue information. A graphical summary of the rogue mobility trend is displayed.
	Rogue Summary See <i>“Rogue Summary” on page 256</i>	Summarizes the rogue device information on the trend of the number of rogues reported on a per controller basis, per hour. The rogue APs and rogue station count is displayed. A graphical summary of the trend on rogue AP, trend on rogue station, and trend on controllers is displayed.
	Top Radio See <i>“Top Radio” on page 258</i>	Provides the Top N radios based on station count, throughput, and high airtime utilization.
Inventory Reports	Access Points Inventory See <i>“Access Points Inventory” on page 259</i>	Lists and tracks all the access points, with its model and software versions on the network.
	Controller Inventory See <i>“Controller Inventory” on page 260</i>	Lists and tracks all the controllers, with its model and software versions on the network.
	Device Availability See <i>“Device Availability” on page 261</i>	Lists all the controllers and access points with its availability, uptime and down time of each of them.
Network Health Reports	Alarm Report See <i>“Alarm Report” on page 262</i>	Lists the total number of critical, major and minor alarms raised on the network. A graphical summary of the alarms distribution by category and top 10 controllers and access points with high alarms is displayed.
	Network Utilization and Capacity See <i>“Network Utilization and Capacity” on page 264</i>	Displays the classification of APs capacity and consumption based on the data throughput and station count for 2.4 GHz and 5GHz channels. The aggregate usage of all selected APs for 2.4 GHz and 5GHz channels are computed as a percentage of total capacity.

TABLE 1: *Supported Report Types*

Category	Report Type	Description
Service Reports	Service Usage Summary See “ Service Usage Summary ” on page 266	Provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.
	Service Usage Trend See “ Service Usage Trend ” on page 267	Provides the service usage trends based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.

Scope

This section allows you to define the scope of a report by performing the device selection followed by the *Service (SSID) Selection*.

Device Selection

The device selection provides the following options:

Field	Description
Default:	By choosing default, report is generated for all the controllers mapped to the nms-server.
Controllers	<ul style="list-style-type: none">• Choose the <i>Controllers</i> option and click on the <i>Select</i> link.• The <i>Controller</i> pop-up provides you a list of all controllers located within the network.• Select one or multiple <i>Controllers</i> and click on <i>OK</i>.• The selected controllers are displayed in the <i>Controllers</i> text box.
Controller Groups	<ul style="list-style-type: none">• Choose the <i>Controller Groups</i> option and click on the <i>Select</i> link.• The <i>Controller</i> Group pop-up provides you a list of all controller groups located within the network.• Select one or multiple <i>Controller Group</i> and click on <i>OK</i>.• The selected controller groups are displayed in the <i>Controller Groups</i> text box.
AP	<ul style="list-style-type: none">• Choose the <i>AP</i> option and click on the <i>Select</i> link.• The <i>AP</i> pop-up provides you a list of all APs located within the network.• Select one or multiple <i>APs</i> and click on <i>OK</i>.• The selected APs are displayed in the <i>AP</i> text box.
AP Groups	<ul style="list-style-type: none">• Choose the <i>AP Groups</i> option and click on the <i>Select</i> link.• The <i>AP Groups</i> pop-up provides you a list of all AP groups located within the network.• Select one or multiple <i>AP Groups</i> and click on <i>OK</i>.• The selected AP groups are displayed in the <i>AP Group</i> text box.

Field	Description
Station Groups	<ul style="list-style-type: none"> Choose the <i>Station Groups</i> option and click on the <i>Select</i> link. The <i>Station Groups</i> pop-up provides you a list of all station groups located within the network. Select one or multiple <i>Station Groups</i> and click on <i>OK</i>. The selected station groups are displayed in the <i>Station Group</i> text box. This option allows you to select station group profiles for which the report must be generated. On generating a station report, the data is displayed only those stations which meet the below criterion: <ul style="list-style-type: none"> Stations must comprise the same 3 byte MAC prefix as the members in the group profile. Stations whose MAC Address completely matches with the member in the group profile.

Service (SSID) Selection

- Click on the *Select* link to select a *Service SSID*.
- The *SSID* pop-up provides you a list of SSIDs.
- Select the SSIDs and click on *OK*.
- The selected SSID is displayed on the *Service (SSID)* text box.

Reporting Interval

These fields depict the time period to be covered by the selected report. These fields are supported for most report types. When these fields do not appear, the report considers the current status. Select the *Schedule* option of the *Recurrence* section, the following options in the *Reporting Interval* section is enabled:

- Last one day:** Select the *Last one day* option. The last one day's report is generated.
- Last one week:** Select the *Last one week* option. The last one week's report is generated.
- Last one month:** Select the *Last one month* option. The last one month's report is generated.
- Interval:** Select the *Interval* option. The report for the given interval period is generated.
 - From* time: The format followed is the mm/dd/yyyy and hh:mm:ss format. The time can be entered manually or by selecting the *Calendar* button.

- *To time.* The format followed is the mm/dd/yyyy and hh:mm:ss format. The time can be entered manually or by selecting the *Calendar* button.



The *Inventory Report* category inclusive of the *Access Point Inventory* and *Controller Inventory* report types consider the present time.

Recurrence

This section allows you to select the time of recurrence. The options are:

- *One Time:* Instant report is generated for the selected reporting interval.
- *Schedule:* This option allows you to define a specific time for report creation. These schedule fields establish the time that a report runs, independent of the *Scope* and *Reporting Interval*.
 - *Daily:* This option allows you to generate daily reports.
 - *Weekly:* This option allows you to generate weekly reports, select *Weekly* option followed by selecting the day of the report generation from the *Every* drop-down list:
 - Monday
 - Tuesday
 - Wednesday
 - Thursday
 - Friday
 - Saturday
 - Sunday
 - *Monthly:* This option allows you to generate monthly reports, select *Monthly* option and enter the *Day of month*; 1-31 is the valid range.

Report Generation Options

To generate a report, select the fields as mentioned in the above from the *Basic Information*, *Recurrence*, *Reporting Level* and *Scope* sections.

Select the following options in the *Report Generation Options*:

- *File Format:* Choose one of the following *Report Generation* file format.
 - *HTML Report:* Select the *HTML* option to export and save the report to HTML format. The generated report is saved with the naming convention *<report type>_report_datetime.html*.
 - *PDF Report:* Select the *PDF* option to export and save the report to PDF format. The generated report is saved with the naming convention *<report type>_report_datetime.pdf*.

- *Email To*: Provide an *Email ID* to email a soft copy of the report in the selected file format. Enter email addresses separated by commas when using multiple email addresses.
- *Customize*: The *Customize Report* option allows you to generate customized reports by selecting the desired attributes to be displayed on the report.
 - Select the *Customize* link. The *Customize Report* pop-up displays the following options:
 - *Display Summary Graphs*: The *Display Summary Graphs* provides the following options:
 - *Yes*: This option displays the graph in the generated report.
 - *No*: This option does not display the graph in the generated report.
 - *Available Attributes*: This column displays a list of available attributes that can be selected for report generation.
 - *Attributes to be displayed in report*: This column displays a list of selected attributes to be displayed in report.

Select the attributes from the *Available Attributes* column and move to the *Attributes to be displayed* in report column.

Select *Save* to customize the report.

- Click *Save*, to save the report in either of the file formats.
- To view the completed report, click *Reports > View Reports*.

Station Reports

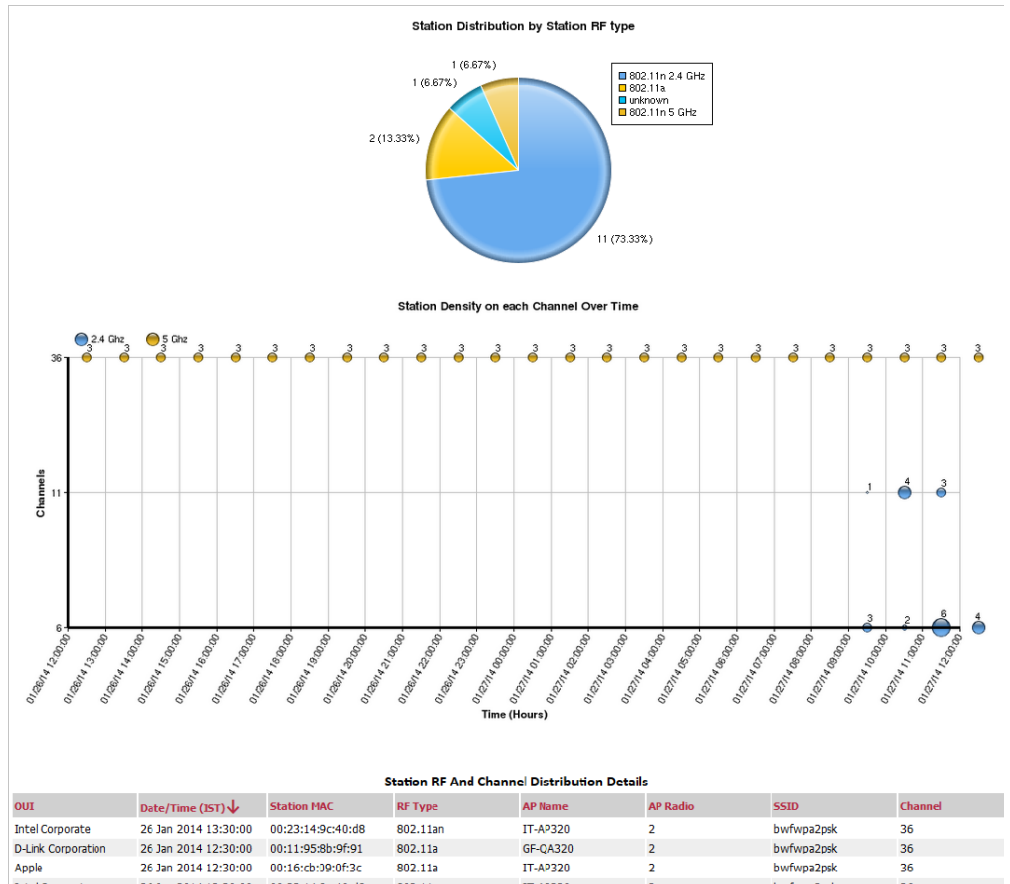
Station RF and Channel Distribution

The *Station RF and Channel Distribution* report type generates reports based on the cumulative statistical data over the reporting interval. It provides the station RF and channel distribution based on OUI. The number of stations per channel over the reporting period with the graphical pie-chart summaries is displayed. Perform these steps to view the most recent version of the *Station RF and Channel Distribution Report*.

1. Navigate to the *Reports > View Reports* screen.
2. Select the *Station RF and Channel Distribution* report type to display the report. The primary sections of this report are as follows:
 - **Graphs**
 - **Station Distribution by RF Type**: Displays the station distribution based on the RF type. For example., 802.11n 2.4 GHz, 802.11a, 802.11n 5 GHz, and Unknown. The categories having less than 5% of total value are clubbed together as *Others*.
 - **Station Density on each Channel Over Time**: Displays the station density on each of the “channels over time” plotted against the selected time range.
 - **Station RF and Channel Distribution Details**: Displays each station's *OUI*, *Date/Time (GMT)*, *Station Mac*, *RF Type*, *AP Name*, *AP Radio*, *SSID* and *Channel*.

Figure 92 on page 250 illustrates the *Station RF and Channel Distribution* report type.

Figure 92: *Station RF and Channel Distribution* report



Station Session Details

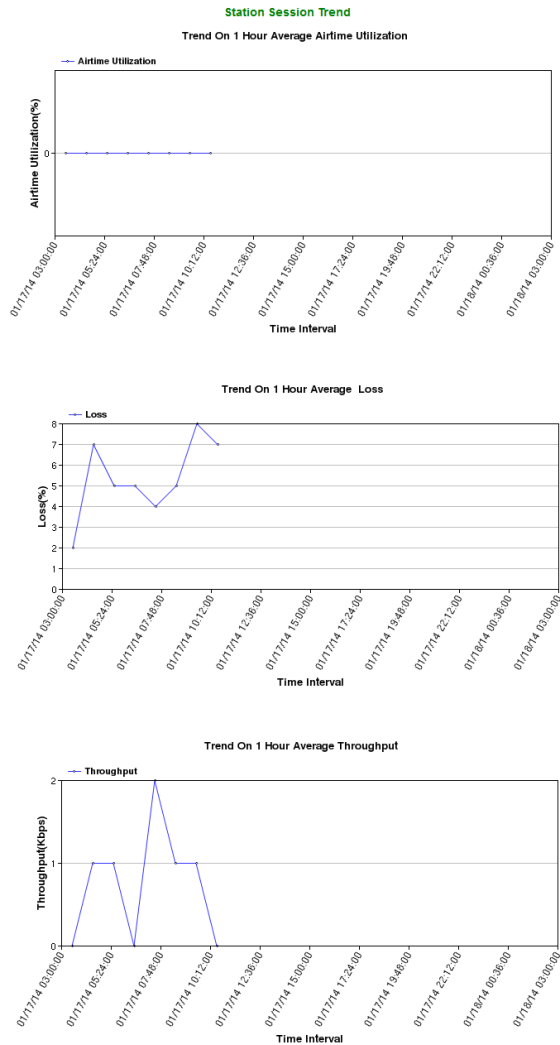
The *Station Session Details* report type provides the average station session trend (*Throughput, Loss, and Airtime Utilization*) for a connected station. Perform these steps to view the most recent version of the *Station Session Details* report.

1. Navigate to the *Reports > View Reports* screen.
2. Select the *Station Session Details* report type to display the report. The primary sections of this report are as follows:
 - **Graphs**
 - **Trend On Airtime Utilization:** Displays the *Airtime Utilization* trend for the selected station.

- **Trend On Loss:** Displays the *Loss* trend for the selected station.
- **Trend On Throughput:** Displays the *Throughput* trend for the selected station.
- **Station Session Details:** This section provides each station's *Date/Time*, *IPV4 Address*, *IPV6 Address*, *Controller*, *AP ID*, *SSID*, *User*, *Throughput (Kbps)*, *Loss%*, *Airtime Utilization%*, and *AP Name*.

Figure 93 on page 251 illustrates the *Station Session Details* report type.

Figure 93: *Station Session Details* report



Station Session Details										
Date/Time (IST)↓	IPv4 Address	IPv6 Address	Controller	AP ID	SSID	User	Throughput (Kbps)	Loss (%)	Airtime Utilization (%)	AP Name
17 Jan 2014 04:39:49	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	3	0	GF-QA320
17 Jan 2014 04:29:48	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	0	0	GF-QA320
17 Jan 2014 04:19:51	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	0	0	GF-QA320
17 Jan 2014 04:09:49	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	0	0	GF-QA320
17 Jan 2014 03:59:47	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	3	0	GF-QA320
17 Jan 2014 03:49:51	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	7	0	GF-QA320
17 Jan 2014 03:39:49	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	3	0	GF-QA320
17 Jan 2014 03:29:48	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	0	0	GF-QA320
17 Jan 2014 03:19:51	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	3	0	GF-QA320
17 Jan 2014 03:09:50	172.16.16.36	0.0.0.0	172.16.16.16	19	bwfwpa2psk		0	3	0	GF-QA320

Top Stations

The *Top Stations* report type generates reports for the top interfering stations based on the *Throughput* and *Airtime Utilization*. The default number of stations displayed is 100. This report type generates the top N stations based on the number of bytes transferred and received and total Rx/Tx. Perform these steps to view the most recent version of the *Top Stations* report.

1. Navigate to the *Reports > View Reports* screen.
2. Select *Top Stations* report type to display the report.
3. The information includes each station's *Station MAC*, *Controller*, *AP Id*, *SSID*, *Throughput (Kbps)*, *Airtime Utilization(%)*, and *Date/Time (GMT)*.

Figure 94 on page 253 illustrates the *Top Stations* report type.

Figure 94: *Top Stations report*

Top 100 Stations with High Throughput					
Station Mac	Controller	AP Id	SSID	Throughput (Kbps) ↓	Date/Time (GMT)
68:ed:43:65:e5:b7	172.16.16.16	26	bwfwpa2psk	0	27 Jan 2014 08:00:00
84:85:06:74:29:5a	172.16.16.16	8	bwfwpa2psk	0	27 Jan 2014 04:00:00
a8:fa:d8:ed:de:11	172.16.16.16	23	bwfwpa2psk	0	27 Jan 2014 15:00:00
b8:b4:2e:91:08:e3	172.16.16.16	20	bwfwpa2psk	0	27 Jan 2014 08:00:00
c0:65:99:4c:4e:ad	172.16.16.16	23	bwfwpa2psk	0	27 Jan 2014 13:00:00
f8:5f:2a:09:b5:ad	172.16.16.16	25	bwfwpa2psk	0	27 Jan 2014 06:00:00
Top 100 Stations with High Airtime Utilization					
Station Mac	Controller	AP Id	SSID	Airtime Utilization(%) ↓	Date/Time (GMT)
00:16:cb:09:0f:3c	172.16.16.16	20	bwfwpa2psk	17	27 Jan 2014 08:00:00
00:23:14:9c:40:d8	172.16.16.16	20	bwfwpa2psk	4	26 Jan 2014 23:00:00
00:11:95:8b:9f:91	172.16.16.16	19	bwfwpa2psk	0	27 Jan 2014 03:00:00
00:21:6a:9e:b8:36	172.16.16.16	23	bwfwpa2psk	0	27 Jan 2014 15:00:00
00:40:96:a3:19:6f	172.16.16.16	20	bwfwpa2psk	0	27 Jan 2014 14:00:00

Unique Stations

The *Unique Stations* report type generates reports based on all stations connected to a network within the reporting interval. A *Unique Station* report is available to all groups and stations connected to network in the selected time range. The unique station details with the graphical pie-chart summaries are displayed. Perform these steps to view the most recent version of the *Unique Stations* report.

1. Navigate to the *Reports > View Reports* screen.
2. Select the *Top Stations* report type to display the report. The primary sections of this report are as follows:
 - **Summary:** Displays the total number of *Unique Stations*.
 - **Graphs:**
 - **RF Band Distribution:** Displays the station distribution based on the RF Type. For example., 802.11n 2.4 GHz, 802.11a, 802.11n 5 GHz, and Unknown. The categories having less than 5% of total value are clubbed together as *Others*.
 - **OUI Distribution:** Displays the station distribution based on the OUI.

- **Device Type Distribution:** Displays the station distribution based on the *Device Type*.
- **OS Distribution:** Displays the station distribution based on the *OS Type*.

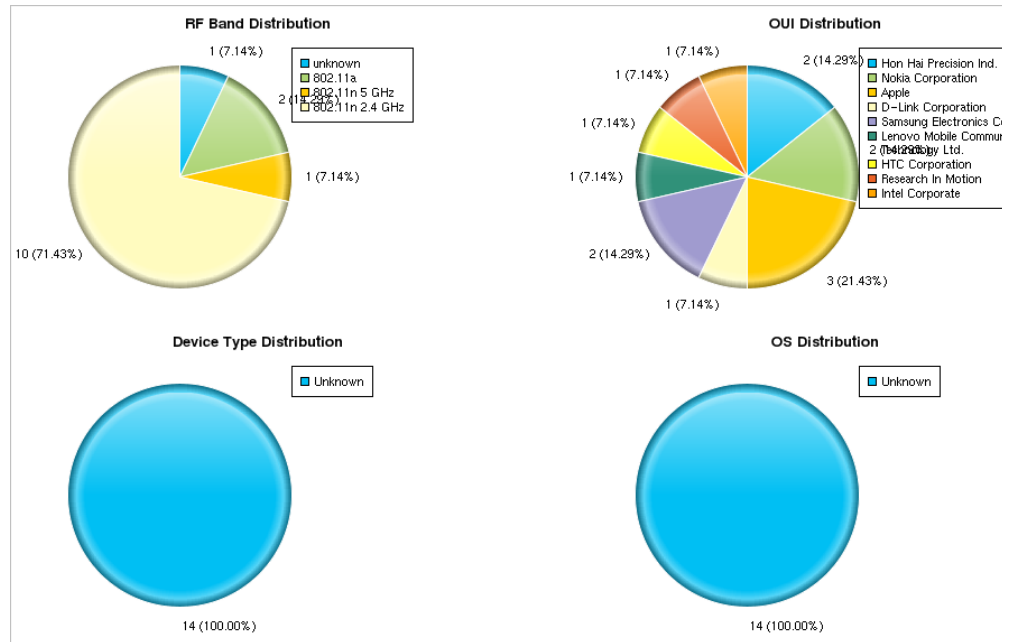


The *Device Type Distribution* and *OS Distribution* pie-graphs displays as *unknown*, if controllers below 6.0 version is mapped to the nms-server. The controllers below version 6.0 do not support the *device finger printing* feature

- **Unique Station Details:** Displays the station's *OUI*, *Date/Time (CST)*, *Station MAC*, *User*, *IPv4 Address*, *IPv6 Address*, *RF Type*, *SSID*, *Device Type*, *OS Type*, and *Floor*.

Figure 95 on page 254 illustrates the *Unique Stations* report type.

Figure 95: Unique Stations report



Unique Stations Details										
OUI	Date/Time (IST) ↓	Station MAC	User	IPv4 Address	IPv6 Address	RF Type	SSID	Device Type	OS Type	F
D-Link Corporation	27 Jan 2014 12:57:56	00:11:95:8b:9f:91		172.16.16.33	0.0.0.0	802.11a	bwfwpa2psk	Unknown	Unknown	
Apple	27 Jan 2014 12:57:56	00:16:cb:09:0f:3c		172.16.16.39	0.0.0.0	802.11a	bwfwpa2psk	Unknown	Unknown	
Intel Corporate	27 Jan 2014 12:57:56	00:23:14:9c:40:d8		172.16.16.59	0.0.0.0	802.11an	bwfwpa2psk	Unknown	Unknown	
HTC Corporation	27 Jan 2014 12:57:56	18:87:96:63:f5:a3		172.16.16.14	0.0.0.0	802.11gn	bwfwpa2psk	Unknown	Unknown	
Research In Motion	27 Jan 2014 12:57:56	68:ed:43:65:e5:b7		0.0.0.0	0.0.0.0	802.11gn	bwfwpa2psk	Unknown	Unknown	
Samsung Electronics Co.,Ltd	27 Jan 2014 12:57:56	a4:eb:d3:6b:ae:75		172.16.16.34	0.0.0.0	802.11gn	bwfwpa2psk	Unknown	Unknown	
Lenovo Mobile Communication Technology Ltd.	27 Jan 2014 12:47:54	c8:dd:c9:d6:79:38		172.16.16.21	0.0.0.0	802.11gn	bwfwpa2psk	Unknown	Unknown	

AP Reports

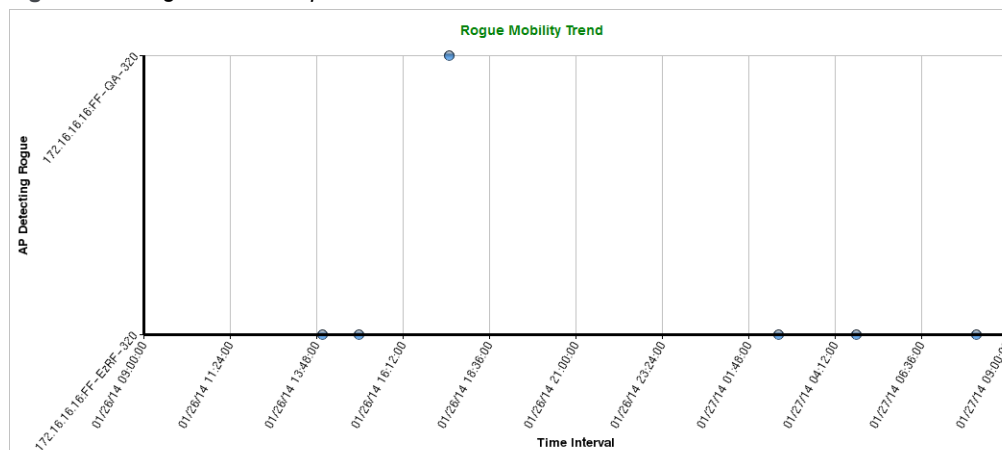
Rogue Details

The *Rogue Details* report type generates individual rogue report. It displays the rogue mobility trend. The trend is plotted against time and APs detecting the rogue. A maximum of hourly data sample is displayed. Perform these steps to view the most recent version of the *Unique Stations* report.

1. Navigate to the *Reports > View Reports* screen.
2. Choose the *AP Reports* category. Select the *Rogue Details* report type to display the report. The primary sections of this report are as follows:
 - **Summary:** Displays the details of the selected rogue.
 - **Graph:** Displays the *Rogue Mobility Trend* graph. The trend is plotted against AP which detects rogues with high strength and its time as samples.
 - **Rogue Details:** Displays the details of the APs detecting rogue along with *Date/Time*, *Controller*, *AP Detecting Rogue*, *AP Location*, *SSID*, *Channel* and *RSSI(dBm)*.

Figure 96 on page 256 illustrates the *Rogue Details* report type.

Figure 96: Rogue Details report



Rogue Details					
Date/Time (IST) ↑	Controller	AP Detecting Rogue	AP Location	Channel	RSSI (dBm)
26 Jan 2014 13:58:04	172.16.16.16	FF-EzRF-320		7	-35
26 Jan 2014 14:58:04	172.16.16.16	FF-EzRF-320		36	-46
26 Jan 2014 17:28:03	172.16.16.16	FF-QA-320		108	-54
27 Jan 2014 02:38:01	172.16.16.16	FF-EzRF-320		100	-36
27 Jan 2014 04:47:57	172.16.16.16	FF-EzRF-320		100	-39
27 Jan 2014 08:07:59	172.16.16.16	FF-EzRF-320		36	-50

Rogue Summary

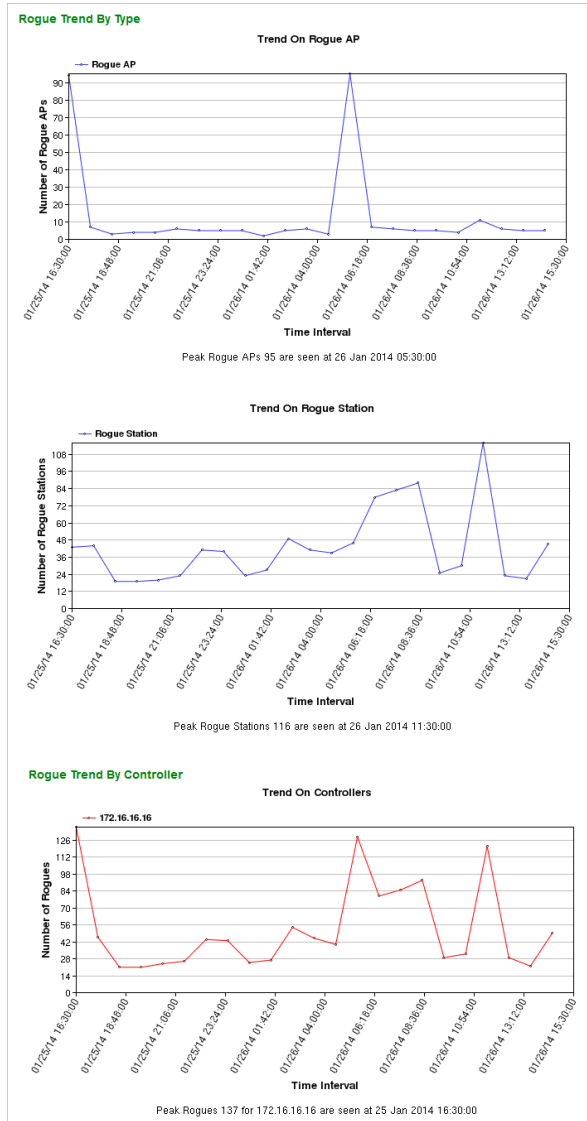
The *Rogue Summary* report type generates reports based on the number of rogues reported on a per controller basis, per hour. Perform these steps to view the most recent version of the *Rogue Summary* report.

1. Navigate to the *Reports > View Reports* screen.
2. Select the *Rogue Summary* report type to display the report. The primary sections of this report are as follows:
 - **Summary:** Displays the details of the total number of rogues.
 - **Graph:**
 - **Rogue Trend By Type:** The *Rogue Trend By Type* graph is categorized as follows:
 - **Trend On Rogue AP:** Displays the trend type based on the number of *Rogue APs*.
 - **Trend on Rogue Station:** Displays the trend type based on the number of *Rogue Stations*.
 - **Rogue Trend By Controllers:** This graph displays the top 10 controllers with the highest number of *Rogues*.

- **New Rogues Detected During Reporting Interval:** Displays the details of new rogues detected during reporting interval with the *Date/Time*, *Controller*, *AP Detecting Rogue*, *AP Location*, *Rogue MAC*, *Rogue Type*, *Wired Rogue*, *Channel*, and *RSSI (dBm)*.

Figure 97 on page 257 illustrates the *Rogue Summary* report type.

Figure 97: *Rogue Summary* report



New Rogues Detected During Reporting Interval								
Date/Time (IST)	Controller	AP Detecting Rogue	AP Location	Rogue MAC	Rogue Type	Wired Rogue	Channel	RSSI (dBm) ↑
No record found								
Rogues Found During Reporting Interval								
Date/Time (IST)	Controller	AP Detecting Rogue	AP Location	Rogue MAC	Rogue Type	Wired Rogue	Channel	RSSI (dBm) ↑
26 Jan 2014 00:28:14	172.16.16.16	FF-QA-320		24:b9:7b:06:f2:93	Station	No	100	-108
26 Jan 2014 06:38:08	172.16.16.16	FF-QA-320		86:fd:8f:b1:f1:f6	Station	No	100	-108
26 Jan 2014 04:18:11	172.16.16.16	FF-QA-320		d0:15:b2:32:17:14	AP	No	36	-108
25 Jan 2014 22:18:13	172.16.16.16	GF-confAP320		00:af:41:2c:00:12	AP	No	36	-106
26 Jan 2014 09:48:09	172.16.16.16	GF-confAP320		3c:c2:f7:6c:88:02	Station	No	36	-105

Top Radio

The *Top Radio* report type generates reports displaying all the top N radios based on *Station Count*, *Throughput*, and *High Loss*. The default number of stations displayed is 100. Perform these steps to view the most recent version of the *Top Radio* report.

1. Navigate to the *Reports > View Reports* screen.
2. Select *Top Radio* report type to display the report.
3. The details of the *AP Name*, *Radio*, *Controller Name*, *AP Location*, *Station*, *Throughput (Mbps)*, *Loss (%)* and *Date/Time (GMT)* is displayed

Figure 98 on page 259 illustrates the *Top Radios* report type.

Figure 98: *Top Radios report*

Top 100 Radios based on Station Count					
AP Name	Radio	Controller Name	AP Location	Station ↓	Date/Time (IST)
GF-QA320	1	172.16.16.16		3	27 Jan 2014 11:30:00
GF-QA320	2	172.16.16.16		3	27 Jan 2014 16:30:00
IT-AP320	2	172.16.16.16		3	27 Jan 2014 19:30:00
GF-confAP320	1	172.16.16.16		3	27 Jan 2014 11:30:00
FF-QA-320	1	172.16.16.16		2	27 Jan 2014 16:30:00

Top 100 Radios based on Throughput					
AP Name	Radio	Controller Name	AP Location	Throughput (Mbps) ↓	Date/Time (IST)
IT-AP320	2	172.16.16.16		2.678	27 Jan 2014 14:30:00
GF-QA320	1	172.16.16.16		0.254	27 Jan 2014 13:30:00
GF-confAP320	1	172.16.16.16		0.215	27 Jan 2014 13:30:00
GF-QA320	2	172.16.16.16		0.174	27 Jan 2014 14:30:00
FF-QA-320	1	172.16.16.16		0.053	27 Jan 2014 11:30:00

Top 100 Radios with High Loss					
AP Name	Radio	Controller Name	AP Location	Loss (%) ↓	Date/Time (IST)
IT-AP320	1	172.16.16.16		48	27 Jan 2014 17:30:00
GF-QA320	1	172.16.16.16		42	27 Jan 2014 11:30:00
FF-Dev320	1	172.16.16.16		41	27 Jan 2014 18:30:00

Inventory Reports

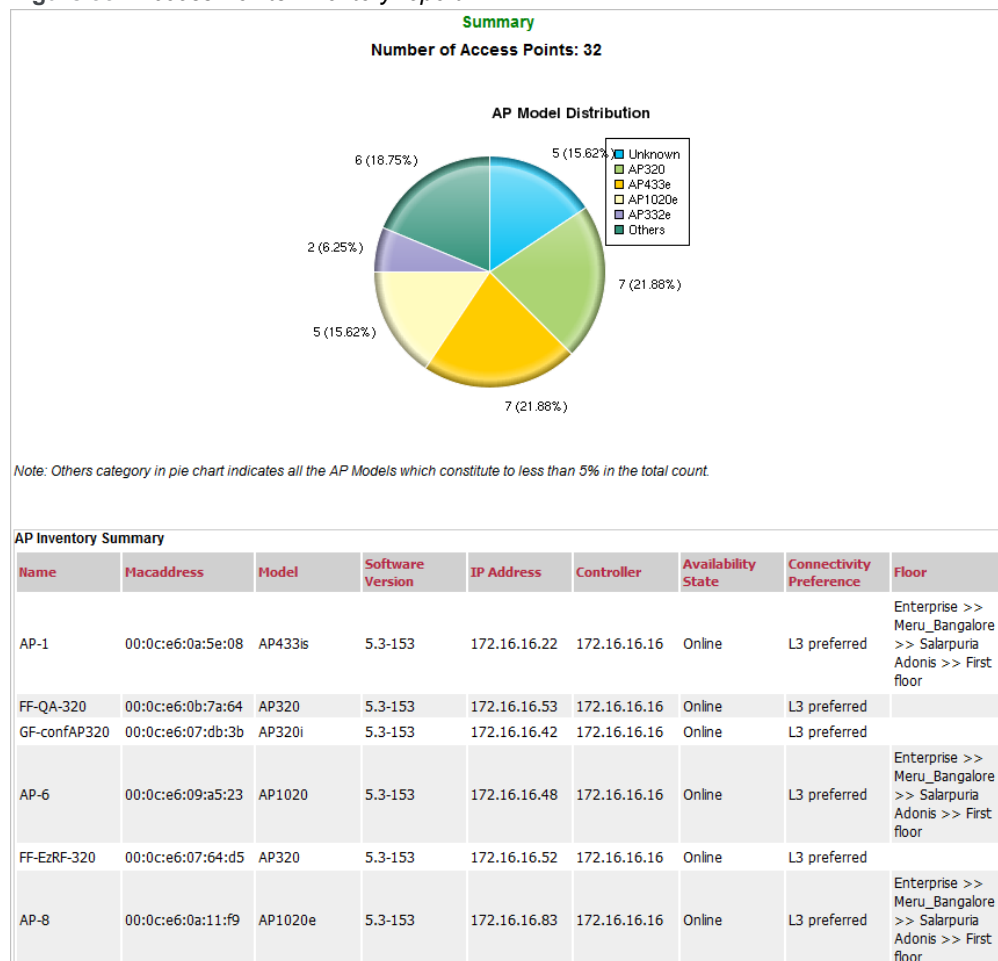
Access Points Inventory

The *Access Points Inventory* report type generates the *AP Inventory Summary* which allows you to track all the access points, with its model and software versions on the network. Perform these steps to view the most recent version of the *Access Points Report*.

1. Navigate to the *Reports > View Reports* screen.
2. Select *Access Points Inventory* report type to display the report. The primary sections of this report are as follows:
 - **Summary:** Displays the total number of access points.
 - **Graph:** Displays the *AP Model Distribution* graph which depicts the distribution of access points.
 - **AP Inventory Summary:** Displays the details of access point inventory such as *Name*, *MAC address*, *Model*, *Software Version*, *IP Address*, *Controller*, *Availability State*, *Connectivity Preference* and *Floor*.

Figure 99 on page 260 illustrates the *Access Points Inventory* report type.

Figure 99: Access Points Inventory report



Controller Inventory

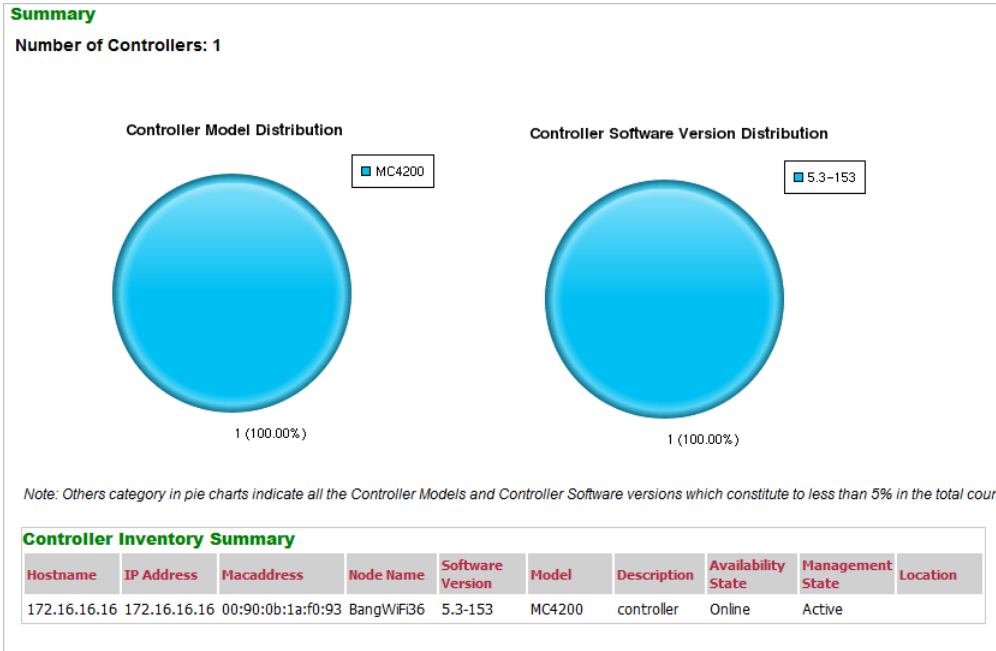
The *Controller Inventory* report type generates the *Controller Inventory Summary* which allows you track all the controllers, with its model and software versions on the network. Perform these steps to view the most recent version of the *Controller Inventory* report.

1. Navigate to the *Reports > View Reports* screen.
2. Select *Controller Inventory* report type to display the report. The primary sections of this report are as follows:
 - **Summary:** Displays the total number of controllers.
 - **Graph:**

- **Controller Model Distribution:** Displays the controllers based on the controller model distribution.
- **Controller Software Version Distribution:** Displays the controllers based on the controller software version distribution.
- **Controller Inventory Summary:** Displays the details of controller inventory such as *Hostname, IP Address, MAC address, Node Name, Software Version, Model, Description, Availability State, Management State* and *Location*.

Figure 100 on page 261 illustrates the *Controller Inventory* report type.

Figure 100: *Controller Inventory* report



Device Availability

The *Device Availability* report type provides you a list of controllers and access points with its availability. It displays the *Device Name, Controller, Availability(%)*, *Uptime*, and *Offline Time of the AP and Controller*.

Figure 101 on page 262 illustrates the *Device Availability* report type.

Figure 101: *Device Availability report*

Device Availability Details				
Device Name	Controller	Availability (%) ↑	Uptime	Offline Time
AP-10	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-29	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-37	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-33	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-28	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-2	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-5	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-36	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-30	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-14	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s
AP-3	172.16.16.16	0	0d: 0h: 0m :0s	0d: 24h: 0m: 0s

Network Health Reports

Alarm Report

The *Alarm* report type generates reports based on the total number of critical, major and minor alarms raised on the network. A graphical summary of the alarms distribution by category and top 10 controllers and access points with high alarms is displayed. Perform these steps to view the most recent version of the *Alarm Report*.

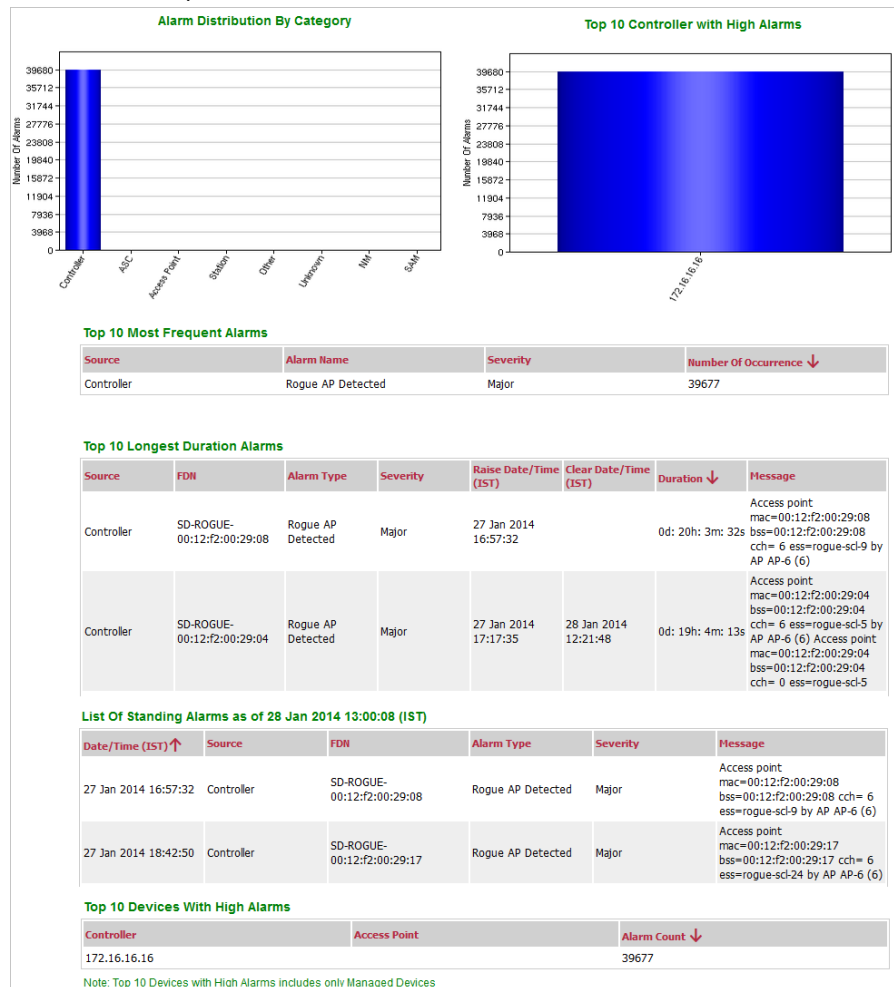
1. Navigate to the *Reports > View Reports* screen.
2. Choose the *Network Health Reports* category. Select the *Alarm* report type to display the report. The primary sections of this report are as follows:
 - **Summary:** Displays the total number of alarms raised. This includes the critical alarms, major alarms and minor alarms.
 - **Graph:**
 - **Alarm Distribution By Category:** Displays the alarm distribution based on category.
 - **Top 10 Controller with High Alarms:** Displays the alarm distribution based on the controller with high alarms.
 - **Top 10 Access Points with High Alarms:** Displays the alarm distribution based on the access points with high alarms.
 - **Alarm Report tables:** The following types of Alarm Reports are generated:
 - **Top 10 Most Frequent Alarms:** Displays the statistical output of the top 10 most frequent alarms raised with details such as *Category*, *Alarm Type*, *Severity*, and *Number of Occurrence*.
 - **Top 10 Longest Duration Alarms:** Displays the statistical output of the top 10 longest duration alarms raised with the details such as *Source*, *Device ID*, *Category*,

Alarm Type, Severity, Raise Date/Time (GMT), Clear Date/Time (GMT), Duration, and Message.

- **List of Standing Alarms:** Displays the statistical output of top 10 standing alarms raised with the details such as *Date/Time (GMT)*, *Source*, *Device Name*, *Category*, *Alarm Type*, *Severity*, and *Message*.
- **Top 10 Devices With High Alarms:** Displays a statistical output of the devices with high alarms raised. It displays the *alarms Device* and *Number of Occurrence*.

Figure 102 on page 263 illustrates the *Device Availability* report type.

Figure 102: Alarm report



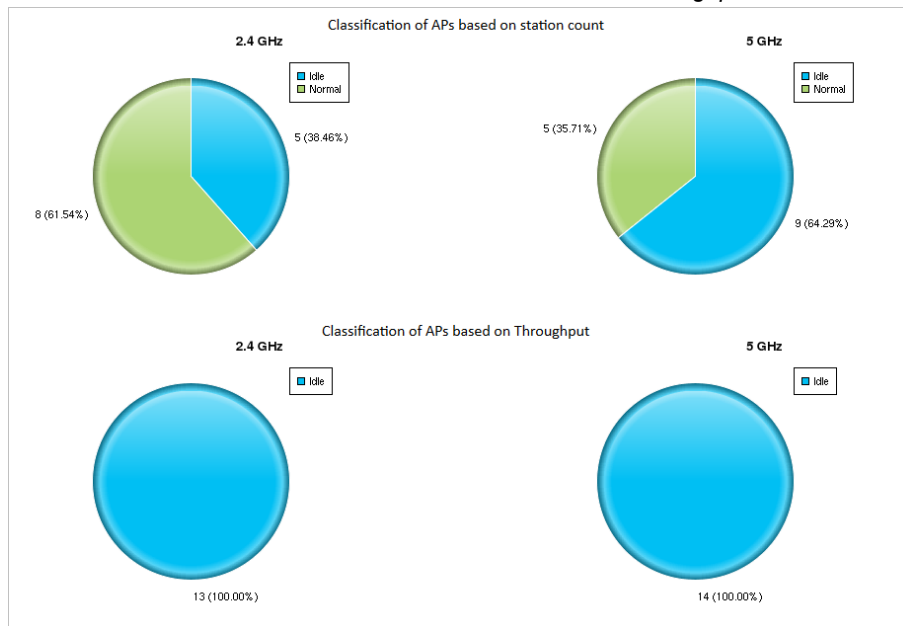
Network Utilization and Capacity

The *Network Utilization and Capacity* report type generates reports based on the overall load of the system. A graphical summary of the classification of APs capacity and consumption based on the data throughput and station count for 2.4 GHz and 5GHz channels is displayed. The aggregate usage of all selected APs for 2.4 GHz and 5GHz channels are computed as a percentage of total capacity. Perform these steps to view the most recent version of the *Alarm Report*.

1. Navigate to the *Reports > View Reports* screen.
2. Select the *Network Utilization and Capacity* report type to display the report. The primary sections of this report are as follows:

Figure 103 on page 264 illustrates the *Classification of APs based on Station Count and Throughput* in the *Network Utilization and Capacity* report type.

Figure 103: Classification of APs based on Station Count and Throughput

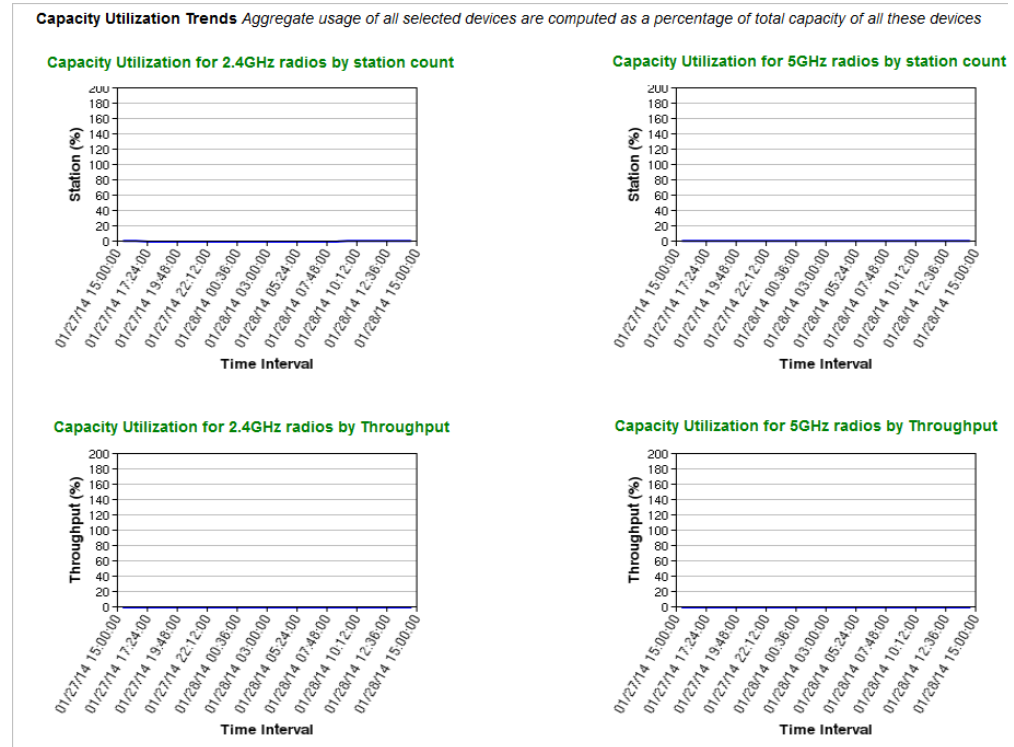


- **Graph:**
 - **Capacity Utilization for 2.4GHz radios by station count:** Displays the capacity utilization for 2.4GHz radios by number of stations.
 - **Capacity Utilization for 5GHz radios by station count:** Displays the capacity utilization for 5GHz radios by the number of stations.
 - **Capacity Utilization for 2.4GHz radios by Throughput:** Displays the capacity utilization for 2.4GHz radios by throughput.

- **Capacity Utilization for 5GHz radios by Throughput:** Displays the capacity utilization for 5GHz radios by throughput.

Figure 104 on page 265 illustrates the *Capacity Utilization Trends* in the *Network Utilization* and *Capacity* report type.

Figure 104: Capacity Utilization Trends



- Network Utilization and Capacity Report tables
 - **List of overloaded APs based on station count:** Displays a statistical output of the list of overloaded APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration > System Administration > Capacity Threshold*). It displays the station's *Controller*, *AP Name*, *AP MAC*, *AP Location*, *AP Model*, *Radio Type*, *Date/Time*, and *Station Count*.
 - List of capacity APs based on station count: Displays a statistical output of the list of capacity APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration > System Administration > Capacity Threshold*). It displays the station's *Controller*, *AP Name*, *AP MAC*, *AP Location*, *AP Model*, *Radio Type*, *Date/Time*, and *Station Count*.
 - List of normal APs based on station count: Displays a statistical output of the list of normal APs based on station count as per the threshold value configured for the particular

AP model in the *Capacity Threshold* screen (*Administration >System Administration > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time, and Station Count*.

- List of idle APs based on station count: Displays a statistical output of the list of idle APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Administration > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time, and Station Count*.
- List of capacity APs based on Throughput: Displays a statistical output of the list of capacity APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Administration > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time, and Station Count*.
- List of normal APs based on Throughput: Displays a statistical output of the list of normal APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Administration > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time, and Station Count*.
- List of idle APs based on Throughput: Displays a statistical output of the list of idle APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Administration > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time, and Station Count*.
- **List of overloaded APs based on Throughput:** Displays a statistical output of the list of overloaded APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Administration > Capacity Threshold*). It displays the throughput's *Date/Time, Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, and Throughput (Mbps)*.

Service Reports

Service Usage Summary

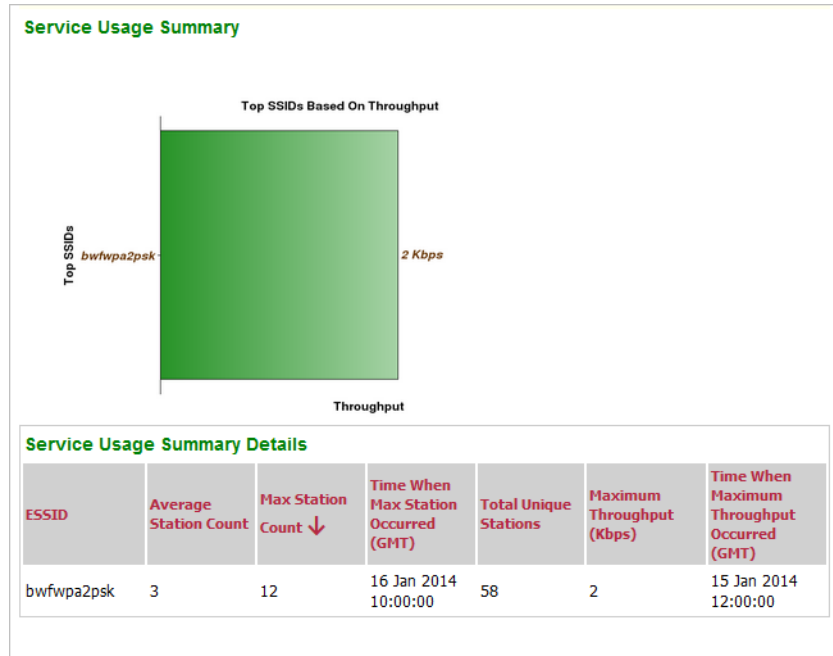
The *Service Usage Summary* report type provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.

1. Navigate to the Reports > View Reports screen.
2. Choose the *Service Reports* category. Select the *Service Usage Summary* report type to display the report. The primary sections of this report are as follows:
 - **Graph:**
 - **Top SSIDs Based on Number Stations:** Displays the top SSIDs based on number of stations.

- **Top SSIDs Based on Throughput:** Displays the top SSIDs based on the throughput.
- **Service Usage Summary:** Displays the *ESSID*, *Average Station Count*, *Max Station Count*, *Time When Max Station Occurred*, *Total Unique Stations*, *Maximum Throughput (Kbps)*, and *Time When Maximum Throughput Occurred (GMT)*.

Figure 105 on page 267 illustrates the *Service Usage Summary* report type.

Figure 105: Service Usage Summary report



Service Usage Trend

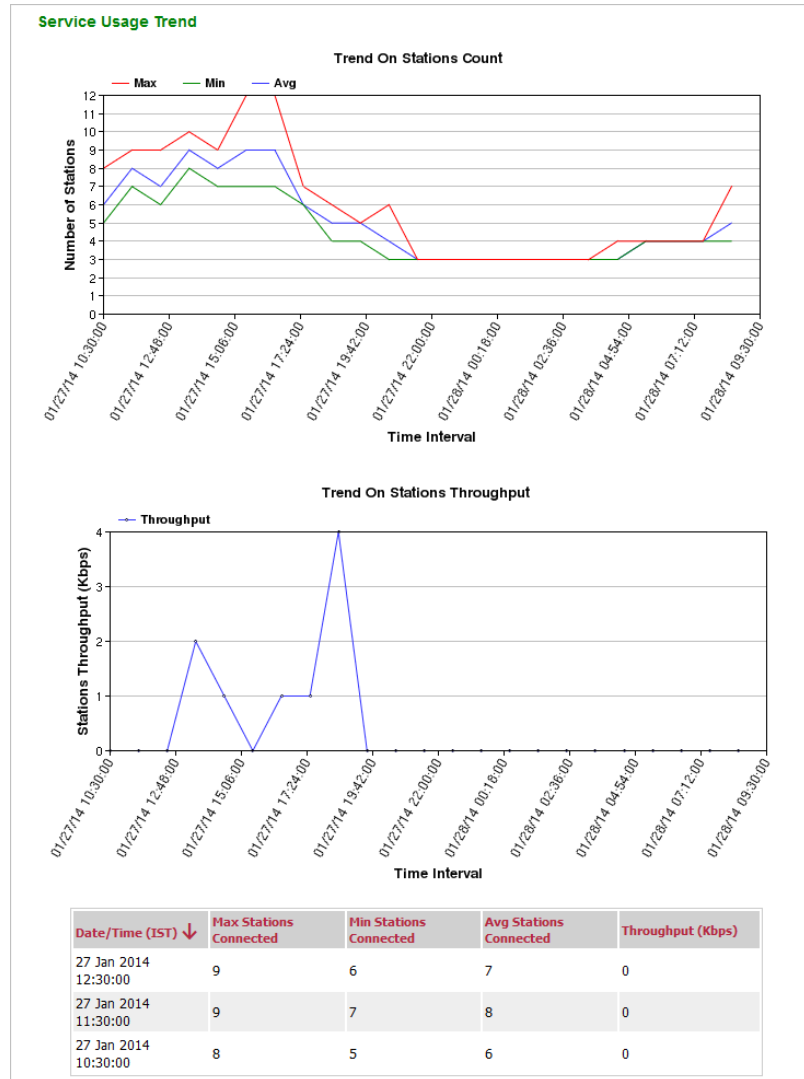
The *Service Usage Trend* report type allows you to generate the service usage trends based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.

1. Navigate to the Reports > View Reports screen.
2. Select the *Service Usage Trend* report type to display the report. The primary sections of this report are as follows:
 - **Graphs:**
 - **Service Usage Trend:** Displays the trend of *Max*, *Minimum* and *Average* stations connected and stations throughput on hourly basis during reporting interval. The graph comprises of three lines, one for *Max* and second one for *Min* and third one for *Average* station count.

- **Trend on Stations Throughput:**
- **Service Usage Trend Details:** Displays the *Date/Time (GMT)*, *Max Stations Connected*, *Min Stations Connected*, *Avg Stations Connected*, and *Throughput (Kbps)*.

Figure 106 on page 268 illustrates the *Service Usage Summary* report type.

Figure 106: *Service Usage Trend* report



View Reports

The *View Reports* screen displays a list of pre-defined reports in *FortiWLM* which are defined in the *Create Reports* screen. It displays the most recent daily version of any report with a single click. Reports in **CSV**, **HTML** or **PDF** format outputs are stored that can be viewed, saved locally, and printed. The *Admin* user can view and edit all report definitions. The users with *monitor* capability can only view the reports and definitions if they have access to all devices in the reports.

1. Click *Reports & Notify > Reports > View Reports*.




























Figure 107 on page 269 illustrates the *View Reports* screen.

Figure 107: View Reports

View Reports

View Reports (11938)

1 - 500 of 11938

REPORT TYPE	NAME	CREATION TIME	FILE FORMAT	STATUS	SIZE(KB)	ACTIONS
<input type="checkbox"/> Rogue Summary	SR_4PM	25 Nov 2013 16:00:28	HTML	Completed	7668	  
<input type="checkbox"/> Access Point Inventory		25 Nov 2013 16:00:27	HTML	Completed	43	  
<input type="checkbox"/> Unique Stations		25 Nov 2013 16:00:26	HTML	Completed	106	  
<input type="checkbox"/> Unique Stations	SR_4PM	25 Nov 2013 16:00:25	HTML	Completed	106	  
<input type="checkbox"/> Rogue Summary		25 Nov 2013 16:00:24	HTML	Completed	7668	  
<input type="checkbox"/> Rogue Details	SR_4PM	25 Nov 2013 16:00:23	HTML	Completed	7	  
<input type="checkbox"/> Station Session Details	SR_4PM	25 Nov 2013 16:00:21	HTML	Completed	6	  
<input type="checkbox"/> Top Stations	SR_4PM	25 Nov 2013 16:00:21	HTML	Completed	22	  
<input type="checkbox"/> Service Usage Trend	SR_4PM	25 Nov 2013 16:00:20	HTML	Completed	56	  

2. The *View Reports* screen provides a list of reports that have been defined in the *Create Reports* screen. See [“Create Reports” on page 241](#).
3. The *Report Type*, *Name*, *Creation Time*, *File Format*, *Status*, *Size*, and *Action* details for each report type can be viewed.

Scheduled Reports

The *Scheduled Reports* screen displays a list of *current running* reports and *future reports*. For recurring reports, the next run time is displayed. The generated reports are sorted by generation time.

1. Click *Reports & Notify > Reports > Scheduled Reports*.

Figure 108 on page 270 illustrates the *Scheduled Reports* screen.

Figure 108: Schedule Reports

Scheduled Reports

Scheduled Reports (289)					
1 - 289 of 289					
REPORT TYPE	NAME	SCHEDULE	LAST RUN	NEXT RUN	
<input type="checkbox"/> Service Usage Trend	SR_1PM_HTML	Daily At 13:00	25 Nov 2013 13:00:01	26 Nov 2013 13:00:00	
<input type="checkbox"/> Service Usage Trend		Daily At 07:00	25 Nov 2013 07:00:02	26 Nov 2013 07:00:00	
<input type="checkbox"/> Service Usage Summary	SR_7AM	Daily At 07:00	25 Nov 2013 07:00:02	26 Nov 2013 07:00:00	
<input type="checkbox"/> Network Utilization and Capacity	SR_7AM	Daily At 07:00	25 Nov 2013 07:00:02	26 Nov 2013 07:00:00	
<input type="checkbox"/> Alarm	SR_7AM	Daily At 07:00	25 Nov 2013 07:00:02	26 Nov 2013 07:00:00	
<input type="checkbox"/> Device Availability	SR_7AM	Daily At 07:00	25 Nov 2013 07:00:02	26 Nov 2013 07:00:00	
<input type="checkbox"/> Controller Inventory	SR_7AM	Daily At 07:00	25 Nov 2013 07:00:02	26 Nov 2013 07:00:00	

- It provides the *Report Type*, *Name*, *Schedule*, *Last Run* and *Next Run* details.
- The report can be scheduled for run by providing the next run details. Select Add option, the *Create Reports* screen is displayed. See [“Create Reports” on page 241](#).

Station Groups

The stations are logically grouped based on *Station Device 3 bytes MAC Prefix* or *Station MAC Address*. The stations are grouped to generate station group based reports by selecting the *scope* as *Station Groups* on the *Create Reports* screen.

- Click *Reports & Notify > Reports > Station Groups*. The *Station Groups* screen is displayed.

[Figure 109 on page 270](#) illustrates the *Station Groups* screen.

Figure 109: Station Groups

Station Groups

Station Groups : 13			
GROUP NAME	DESCRIPTION	LAST UPDATED	
<input type="checkbox"/> Gemtek Technology Co., Ltd.	00:1a:73	21 Sep 2012 21:22:21	
<input type="checkbox"/> Motorola Mobility, Inc.		07 Sep 2012 11:44:53	
<input type="checkbox"/> Hon Hai Precision Ind. Co.,Ltd.	90:4ce5	11 Jul 2012 14:55:07	
<input type="checkbox"/> Murata Manufacturing Co., Ltd.	04:46:65	11 Jul 2012 14:54:36	
<input type="checkbox"/> HTC Corporation	f8:db:7f	11 Jul 2012 14:53:50	
<input type="checkbox"/> Research In Motion	68:ed:43	11 Jul 2012 14:53:14	
<input type="checkbox"/> Nokia corporation		11 Jul 2012 14:51:57	
<input type="checkbox"/> samsung electronics corp		11 Jul 2012 14:51:09	
<input type="checkbox"/> apple 1		11 Jul 2012 14:50:07	
<input type="checkbox"/> intel4		11 Jul 2012 14:49:43	
<input type="checkbox"/> intel3		11 Jul 2012 14:48:08	
<input type="checkbox"/> intel2		11 Jul 2012 14:47:41	
<input type="checkbox"/> intel1		11 Jul 2012 14:42:21	

- The *Station Groups* screen displays a list of all *Station Groups*. Each **Station Group** displays the *Group Name*, *Description*, and *Last Updated* details.

3. You can perform the following actions on the *Station Groups* screen by selecting the respective options:
 - Add Station Group - [“Add Station Group” on page 271](#)
 - Edit Station Group - [“Edit Station Group” on page 271](#)
 - Delete Station Group - [“Delete Station Group” on page 271](#)

Add Station Group

The *Add* option allows you to create a *Station Group* by selecting individual stations. The stations are grouped by selecting a list of *MAC Addresses* or by selecting the *MAC Prefixes*.

1. Click on the *Add* icon (+) located on the top right hand side of the *Station Groups* screen.
2. In the *Station Groups-Add* screen you are allowed to create a station group by adding a list of *MAC Addresses* and *MAC Prefixes*.
3. Select *Save*. The new station group is created and displayed on the *Station Groups* screen.

Edit Station Group

The *Edit* option allows you to edit a *Station Group*. Some more stations can be included to the existing group by selecting a list of *MAC Addresses* or by selecting the *MAC Prefixes*.

Delete Station Group

The *Delete* option allows you to delete a *Station Group* from the *Station Groups* screen.

User Preferences

FortiWLM manages and monitors the performance of controllers. The *Notification* option allows you to notify when any NM managed controller goes down. The notification system identifies the alarm corresponding to the controller down condition and forwards the alarm to the user through email. A *notification profile* is set up to indicate the recipients for notification. A *notification filter* is provided to indicate the type of error that triggers notification. To notify via email, set up an *SMTP Server* description. You can schedule email notification to occur regularly or you can send email only when a certain event occurs.

Set Up Email Notification

Complete these four tasks to set up email notification:

- Create a *User on Email*, See [“Create a User on Email” on page 281](#)
- Configure a *Mail Server for Notification*, See [“Configure a Mail Server for Notification” on page 281](#)
- Add a *Notification Profile*, See [“Add a Notification Profile” on page 272](#)

- Add a *FortiWLM Notification Filter*, See [“Add a FortiWLM Notification Filter”](#) on page 272

Add a Notification Profile

A notification profile comprises of a list of email Ids to indicate the error that triggers notification. The profile is created and referenced in *FortiWLM* notification filter or from an application that works with *FortiWLM*, for example *SAM*. You can associate multiple notifications to a single profile when you set up email notification using the notification filter. The filters discovers the names of profiles and displays them in a drop-down list during configuration.

To configure a FortiWLM notification profile, follow these steps:

1. Navigate to *Reports & Notify > User Preference > Notification Profiles > Add*. [Figure 110 on page 272](#) illustrates the *Notification Configuration - Add* screen.

Figure 110: Notification Configuration - Add

Notification Configuration - Add

The screenshot shows a web form titled "Notification Configuration - Add". It contains three main input sections:

- Notification Name:** A text box containing "Test". To its right, it says "[1-32] chars., Required".
- Notification Description:** A text box containing "Testing". To its right, it says "[0-128] chars.".
- E-Mail ID(s)*:** A larger text box containing "abc@merunetworks.com". To its right, it says "[1-1023] chars., Required".

2. In the *Notification Configuration - Add* screen, enter a notification name such as *Critical_Alarm_Messages*.
3. Provide a description for the notification.
4. Provide the email addresses (up to 1024 characters). The following are the methods:
 - List each email address on a new line, such as:
sandy@fortinet.com
mike@fortinet.com
 - Separate the email addresses with commas such as: sandy@fortinet.com, mike@fortinet.com
5. Click Save.
6. You can associate multiple notifications to a single profile when you set up email notification using the notification filter.
7. The existing Notification Profiles can be modified and deleted. The profiles that are used by the filter cannot be deleted, an error message is thrown while deletion.

Add a FortiWLM Notification Filter

A notification filter specifies which alarms trigger notification. For example, if you select critical in the filter, only critical alarms will trigger notification. You can configure the notification filter and send the weekly report. To configure a filter, follow these steps:

1. Navigate to *Reports & Notify > User Preference > Notification Filters > Add*.
2. In *Notification Filters - Add* screen, provide the *Filter Name*, *Filter Description*, *Notification Profile*, and *Filter Status*. See [Figure 111 on page 273](#).

Figure 111: Notification Filters - Add

Notification Filters - Add

Filter Name

Test

[1-32] chars., Required

Filter Description

Testing

[0-128] chars.

Notification Profile

sam6dot1

Filter Status

☐ Inactive
 ☒ Active

Filter Type	Select	Options
Alarm Severity	<input type="checkbox"/>	<input type="checkbox"/> Critical <input type="checkbox"/> Major <input type="checkbox"/> Minor <input type="checkbox"/> Clear
Alarm Severity Change	<input type="checkbox"/>	<input type="checkbox"/> Critical to Clear <input type="checkbox"/> Major to Clear <input type="checkbox"/> Minor to Clear
Include Alarms	<input type="checkbox"/>	<div> AP CPU Usage High AP Down AP Memory Usage High AP Radio Card Failure AP Wireless Interface Down AP Wireless Interface Down due to fallback channel not found AP Wireless Interface Station Capacity Full </div>
Exclude Alarms	<input type="checkbox"/>	<div> AP CPU Usage High AP Down AP Memory Usage High AP Radio Card Failure AP Wireless Interface Down AP Wireless Interface Down due to fallback channel not found AP Wireless Interface Station Capacity Full </div>
Alarm Message	<input type="checkbox"/>	<div></div> <div>[0-256] chars.</div>
Alarm Source	<input type="checkbox"/>	<div></div> <div>IP Address/Hostname [0-256] chars.</div>
Alarm Device	<input type="checkbox"/>	<div></div> <div>MAC/IP Address [0-64] chars.</div>
AP Groups	<input type="checkbox"/>	<div></div> <div> <div>SELECT AP GROUP</div> <div>[0-64] chars.</div> </div>

3. Configure the *Notification Filter* with one or more *Notification Filter Types* listed below. If you select multiple criterion, the alarm should meet all requirements for notification to be sent. For example, if you want only critical alarms from one particular controller, set both *Alarm Severity* and *Alarm Source* as the controller host name.
- **Alarm Severity** – Set this filter based on alarm severity. The values are *Critical*, *Major*, *Minor* and *clear*.

- **Alarm Severity Change** – Set notification to trigger when an alarm clears. The values are *Critical to Clear*, *Major to Clear*, and *Minor to Clear*.
- **Include Alarms** – Set this filter based on the alarms that occur. All the alarms are listed for this field and you can include multiple alarms in one filter set. The available alarms are:
 - AP CPU Usage High
 - AP Down
 - AP Memory Usage High
 - AP Radio Card Failure
 - AP Wireless Interface Down
 - AP Wireless Interface Down due to fallback channel not found
 - AP Wireless Interface Station Capacity Full
 - Controller CPU Usage High
 - Controller down
 - Controller Memory Usage High
 - Controller unreachable
 - DHCP Address Pool Exhausted
 - Fan Module Failure
 - Link Down
 - Master Down
 - Power Module Failure
 - RADIUS Server Failed
 - RAID status
 - Rogue AP Detected
 - Software License Expired
 - Software License Violated
 - System High Temperature
 - Wired Rogue Detected

For detailed information on *configuring Alarms* and *Alarm definitions*, see the **Fault Management** screen (*Monitor > Fault Dashboard > Fault Management*) in *Online Help*.

- **Exclude Alarms** – Exclude these alarms from the filter. All the alarms (see list above) are listed for this field and you can exclude alarms in one filter set. You cannot both include and exclude the same alarm.
- **Alarm Message** – Set the filter based on the substring to be matched in the Alarm message (the filtering is not case sensitive).

- **Alarm Source** – Set this filter based on the controller device that triggered the alarm. Provide an IP address or hostname for a controller.
 - **Alarm Device** – Set this filter based on the source of the AP/device that triggered the alarm. The filter criterion enables you to filter the alarms based on the device on which the alarm is raised. For example, if AP MAC is provided, the alarms for the AP MAC are filtered.
 - **AP Groups** - Select the AP Groups option, the Select AP Groups screen is displayed. Select an AP Group from the hierarchy and click *Save*. The selected AP Group is displayed in the AP Groups section. Each of the AP group consists of APs. A notification message is triggered, for the alarms raised for the APs within the AP Group.
4. Click *Save*.



There is AND operation across Filter Types and OR operation within the Filter Type. For example, if you want to receive all the critical alarms except Rogue alarms, configure the notification filter like this. Include Alarm severity - Critical and exclude Rogue Alarm type from the Exclude Alarms type list. On the other hand, if you want to receive any of the alarms (Critical or Major or Minor, or Clear) set the notification filter to include the “alarm severity” Critical or Major or Minor or Clear.

5. The Notification filters can be modified and deleted.

Service Assurance Manager (SAM) Notification

Notification is also used by FortiWLM’s related applications such as Service Assurance Module (SAM). SAM email notification uses its own filter along with profiles created in *FortiWLM*.

Troubleshooting Notification

The most common notification errors are:

- Including an incorrect email address in an email list
- Selecting incorrect filters in the notification filter

If there is any misconfiguration in the email list, the error “*Failed to send email notification using Primary SMTP server Configuration. Reason: Invalid input data*” is displayed on the *Alarms Dashboard* (Monitor > Fault Management > Fault Dashboard > Alarms).

If the SMTP server supports authentication, configure the email list to identify (and drop) only the incorrect email addresses (see “[Set Up Email Notification](#)” on page 271 to add authentication details to the email configuration). This way, the SMTP server does not try to resolve email ID domain names when the *Alarm Manager* sends a mail to the SMTP server. Only the misspelled email address receives an error and all correct addresses receive the notification. If authentication is not supported and even one email address is incorrect, no users on the mailing list will receive the message. The only way to correct the problem is to remove or correct the email address.

Notification filters can be configured incorrectly if you don't keep in mind that checking filters is an AND/OR operation. For example, when adding a filter, if you checked all of the options for Alarms and Alarms severity, you receive only clear alarms, which is probably not what you intended. In this case, If you wish to receive Rogue AP alarms only, uncheck the options in 'Alarm severity'.

Administrators in different user groups can configure separate notification profiles for the same controller. Since applying a notification alarm is a global operation, you can configure your notifications correctly and still have notification errors if another administrator managing the same controller mis-configures *their* group's notification list on the controller. If there is any misconfiguration in any one of the notification lists for a controller, it affects all notifications for that controller.

8 Administration

System Administration

The *System Administration* allows you to view and configure the following:

- “[Server Parameters](#)” on page 277
- “[Supported Controller Versions](#)” on page 278
- “[Mail Servers](#)” on page 280
- “[SNMP Configuration](#)” on page 282
- “[Capacity Threshold for Radio](#)” on page 285
- “[System Log View](#)” on page 286
- “[FortiWLM Maintenance](#)” on page 289
- “[FortiWLM Diagnostics](#)” on page 293

Server Parameters

The server parameters screen allows you to view the server parameters of the *NM Services Appliance* (SA200, SA250, SA2000).

1. Navigate to *Administration > System Administration > Server Details*.
2. In the *Server Parameters* screen you can view the following details. [Figure 112 on page 278](#) illustrates the *Server Parameters* screen.

Field	Description
Description	Displays the user assigned description for the services appliance. For example, it might include appliance location, such as Building_1, Floor2. This field can be modified.
Public IP Address	Displays the IP address. This field is configurable when the E(z)RF server comprises of public IP address.

Field	Description
Host Name	Displays the services appliance host name assigned by DNS. Typically, administrators maintain the same host name even if the IP Address is changed.
Uptime	Displays the elapsed time since the last reboot.
IP Address	Displays the IP address of the appliance that is used to connect E(z)RF-NM GUI.
Netmask	Displays the subnet mask for the IP address.
Default Gateway	Displays the gateway for the appliance.
DHCP Server	Displays the if the appliance comprises of a static IP address. If it does not comprise of a static IP address, then the DHCP server assigns one.
Software Version	Displays the software version of the NM server.
Server Model	Displays the NM server model number (SA200, SA250 or SA2000)
Manufacturing Serial #	Displays the serial number of the NM server.
System ID	Displays the system ID of the NM server.

Figure 112: Server Parameters

Server Parameters

Description	<input type="text" value="NM Server"/> [0-256] chars.
Public IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Host Name	msraju-SA250
Uptime	06d:08h:26m:38s
IP Address	172.19.44.204
Netmask	255.255.255.0
Default Gateway	172.19.44.1
DHCP Server	0.0.0.0
Software Version	4.0-6-0
Server Model	SA250
Manufacturing Serial #	4212SA2502034
System Id	FD37376FFB11


Supported Controller Versions

Supported Controllers

1. Navigate to *Administration > System Administration > Supported Controllers*.
2. The *Supported controllers* screen provides you a list of *NM* supported controller versions and the supported *NMS Agent Versions*. The controller version mentioned in this screen is the minimum build which is supported by the *FortiWLM*. [Figure 113 on page 279](#) illustrates the *Supported Controllers* screen.

Figure 113: Supported Controllers

Supported Controllers

Supported Controllers Import NMS Agent 	
MINIMUM BUILD OF A CONTROLLER RELEASE ↕	AGENT VERSION ↕
5.0-89	4.0-5.0-A-0
5.1-41	4.0-5.1-A-0
5.1d-80	4.0-5.1-A-0
5.2-40	4.0-5.2-A-0
5.2-53	4.0-5.2-B-0
5.3-50	4.0-5.3-A-0
5.3-101	4.0-5.3-B-0
6.0-175	4.0-6.0-A-0
6.0-1-0	4.0-6.0-A-0

Import NMS Agent tab

An NMS agent is pre-installed onto each controller and that agent becomes part build with no action required on your part. However, if a new agent is created to support a particular new controller version, you need to import the new agent patch by following these steps:

1. Navigate to *Administration > System Administration > Supported Controllers*.
2. In the *Supported Controllers* screen, select the *Import NMS Agent* tab. [Figure 114 on page 280](#) illustrates the *Import NMS Agent - Update* screen.

Figure 114: *Import NMS Agent - Update*

Import NMS Agent - Update

Supported Controllers | **Import NMS Agent**

Step 1 Select a NMS Agent File

- Only Files with the extensions : **.rpm** are allowed.
- The **Browse...** button allows to choose the NMS Agent File you wish to Import.
- **File:**

Step 2 Import the NMS Agent File

- Click **Import NMS Agent** button to start the Import Process.

3. In the *Import NMS Agent - Update* screen, select the *NMS Agent* file that you wish to import by selecting the *Browse* option. Only files with the extensions **.rpm** are allowed.
4. Choose the file and Click *Import NMS Agent* button to start the Import Process.

Mail Servers

When an error occurs, *FortiWLM* can notify you by email. To indicate the error that triggers notification, set up a *Notification Filter*. To indicate who should be notified and how they are notified, set up a *Notification Profile*. To turn notification *on* and *off*, activate or deactivate the filter.

To notify via email, set up an *SMTP Server* description. You can schedule email notification to occur regularly or you can send email only when a certain event occurs.

Set Up Email Notification

Complete the below tasks to set up email notification:

- Create a User on Email, See [“Create a User on Email” on page 281](#)
- Configure a Mail Server for Notification, See [“Configure a Mail Server for Notification” on page 281](#)
- Add a Notification Profile, See [“SNMP Configuration” on page 282](#)
- Add a *FortiWLM* Notification Filter, See [“Add a FortiWLM Notification Filter” on page 272](#)

Create a User on Email

On your email system, create a user like *alert@fortinet.com*. You will use this email user to configure a mail server for notification, add a notification profile, and add a *NM* notification filter.

Configure a Mail Server for Notification

FortiWLM needs mail server information to send automated emails. These servers are used for email notification. To configure the mail server, follow these steps:

1. Navigate to *Administration > System Administration > Mail Servers > Add*. *Figure 115 on page 281* illustrates the *SMTP Server Configuration - Add* screen.

Figure 115: SMTP Server Configuration - Add

SMTP Server Configuration - Add

Server Type	primary	
Server (Hostname/IP address)*	10.0.0.100	[1-256] chars., Required
Server Port*	25	Valid range: [1-65535], Required
From Email Address*	abc@test.com	[1-256] chars., Required
Authentication	No	
SMTP Login Username*	admin	[1-64] chars., Required
SMTP Login Password*	••••••••	[1-64] chars., Required
Use secure connection	No	

2. In the *SMTP Server Configuration - Add* screen, provide the following details.
3. Select primary or secondary for *Server Type*. The *FortiWLM* uses the available primary server.
4. Enter the host name (for example smtp145) or IP Address of the SMTP Server (for example, 10.1.4.5). Each field has a maximum of 256 characters.
5. Indicate which port the *SMTP Server* uses. The default server port is 25. If the SMTP server uses another port, modify this setting (1 - 65535).
6. Enter the *From Email Address* (up to 256 chars). The *From Email Address* is the email address you set up to *Create a User on Email*.
7. If you need authentication to access email, change *No* (default) to *Yes*. If Authentication is set to *Yes*, enter an *SMTP Login Username* (up to 64 chars). Enter the corresponding password (up to 64 chars) in the *SMTP Login Password*.

8. You have the option to use a secure connection to send mail. Set it to *Yes* if the *SMTP Server* is enabled with *Secure Connection*. The default option is *No*.
9. Select *Save*. The mail server configuration is added and displayed on the *SMTP Server Configuration* screen.
10. To update *SMTP Server Configuration* information, click *Refresh*.

SNMP Configuration

Forti WLM supports all versions (SNMPv1, SNMPv2c, and SNMPv3) of SNMP Protocol.



Forti WLM doesn't support write operation through SNMP. You need to provision any required configuration through the web UI.

SNMP displays management data in the form of variables on the managed systems, which describe the system configuration. It uses an extensible design, where the available information is defined by *Management Information Bases* (MIBs). The MIBs describe the structure of the management data of a device subsystem; they comprise a hierarchical name space containing *object identifiers* (OID). Each OID identifies a variable that can be read via SNMP.

MIB Tables

The MIB tables SNMP implementation can be downloaded from NM. The MIB Tables are also available on the Fortinet web site. A summary of the Forti WLM MIB Enterprise tables are:

- mnmControllerInventoryEntry
- mnmControllerStateEntry
- mnmAPEntry
- mnmStationEntry
- mnmApIf80211Entry
- mnmApIf80211statsEntry

Download the MIB Tables for Management Applications


If you are using a third-party SNMP-based *FortiWLM* program, you will need to integrate the Fortinet *NM* proprietary MIB tables that allow the manager program to manage controllers and APs. The MIB tables are available in a compressed (zipped) file that can be copied from the services appliance.

1. Open a Web Browser (IE or Firefox), enter the system IP address (example: <https://172.29.0.133>) and then enter a user name and password (factory default user name/password is admin/admin).
2. Navigate to *Administration > System Administration > SNMP > Download MIBs*.
3. When the download is complete, you will see the file listed in the *Downloads* list.
4. Save the file mibs(x).tar.gz.

Configure SNMP Service on Forti WLM With the Web UI

1. Open a Web Browser (IE or Firefox), enter the system IP address (example: <https://172.29.0.133>) and then enter a *User Name* and *Password* (factory default user name/password is admin/admin).
2. Navigate to *Administration > System Administration > SNMP*.

Figure 116: SNMP Administration

SNMP Administration Enable Auto Refresh 

SNMP Service Status: **Running** STOP RESTART

MIBs	
DOWNLOAD ALL MIBS	
APPLICATION	ACTION
MIB Structure	Download MIB
System Details	Download MIB
Network Manager	Download MIB

SNMP Community Management SNMP V3 User Management

MANAGER IP/HOSTNAME	COMMUNITY STRING	TRAP SUPPORT	TRAP PORT	TRAP VERSION	ACTIONS
<input type="checkbox"/> 172.17.3.37	meru2002	Enable	162	both	Trap Filter
<input type="checkbox"/> 172.16.10.36	meru	Disable			
<input type="checkbox"/> 172.18.124.12	linux	Disable			
<input type="checkbox"/> 172.16.10.51	bangwifi	Disable			

3. The *SNMP Administration* screen allows you to perform the following actions. [Figure 116 on page 283](#) illustrates the *SNMP Administration* screen.

Stop and Restart an SNMP Service

The following two actions can be performed:

- **Stop SNMP:** This allows you to *Stop* the SNMP and its related applications running on the services appliance.
- **Restart SNMP:** This allows you to *Restart* SNMP and its related applications running on the services appliance.

Status of SNMP Service

- **Stopped:** Here, the SNMP and its related applications are Stopped. The SNMP functionality like *SNMP Configuration*, *Trap Forwarding* and *SNMP Get Requests* are disabled.
- **Running:** Here, the SNMP and its related applications are Up and Running. The SNMP functionality like *SNMP Configuration*, *Trap Forwarding* and *SNMP Get Requests* are enabled.

SNMP Registered Applications on Services Appliance

The below include the list of installed applications registered with the SNMP Manager on the services appliance and are listed for SNMP requests:

1. FortiWLM
2. Service Assurance Manager
3. Spectrum Manager
4. WIPS

Download MIBS

Download All MIBS to install all applications and **Download MIBS** to install individual applications is installed on the services appliance.

Configure SNMP Parameters

The **SNMP Parameters enables** you to register the external SNMP Managers with the *Forti-WLM*. The SNMP v1, v2c and v3 versions are supported to receive requests. The v1, v2c and both are supported for trap forwarding. The *SNMP Administration* screen provides the following tabs to configure the SNMP parameters:

- [“SNMP Community Management” on page 284](#)
- [“SNMP V3 User Management” on page 284](#)

SNMP Community Management

The SNMP v1 and v2c requests are diverted to the *SNMP Community Management* tab.

Select *Add* on the *SNMP Community Management* tab. Provide the *Manager IP / Hostname*, *Community String*, *Trap Support*, *Trap Port* and *Trap Version*. Traps for the respective *Manager IP / Hostname* can be filtered by selecting the *Trap Filter* option. The SNMPv1 and v2c traps can be modified or deleted by selecting the respective options. [Figure 116 on page 283](#) illustrates the *SNMP Administration* screen.

SNMP V3 User Management

The *SNMP v3* user configurations are diverted to the *SNMP v3 User Management*.

Select *Add* on the *SNMP v3 User Management* tab. Provide the *Username*, *Authentication Protocol*, *Authentication String*, *Privacy Protocol*, and *Privacy String*. The password of an indi-

vidual *SNMP v3* can be modified by selecting the *Password Reset* option. The *SNMP v3* can be deleted by selecting the respective option. [Figure 117 on page 285](#) illustrates the *SNMP V3 User Management* screen.

Figure 117: SNMP V3 User Management

SNMP Community Management

SNMP V3 User Management

USERNAME

AUTHENTICATION PROTOCOL

PRIVACY PROTOCOL

syslogtest

No Authentication

No Privacy

arun

MD5

No Privacy

vikram

MD5

DES

ezrf_test

SHA

DES

venu_FCS_test

MD5

No Privacy

See the **SNMP Administration** screen (*Administration > System Administration > SNMP*) in Online Help for detailed information on *SNMP Administration* topic.

Capacity Threshold for Radio

The *FortiWLM* supports many controllers and access points which operate on a Fortinet services appliance hardware device or in a virtualized environment based on VMware. Access Points contain radio devices that communicate with the Forti WLC and form the wireless LAN (WLAN). The controllers and access points connect to the site's wired LAN through wired switches. The network utilization is derived from per radio statistics. The *Capacity Threshold for Radio* are *Station Count Range*, *Throughput (Mbps) Range* and *Airtime Utilization(%) Range* values can be modified for each AP model located on the *FortiWLM*. Follow the below mentioned steps to view and modify the Capacity Threshold for Radio:

1. Navigate to *Administration > System Administration > Capacity Threshold*.
2. The *Capacity Threshold for Radio* screen provides the *Station Count Range*, *Throughput (Mbps) Range* and *Channel Utilization(%) Range* values for all AP Models.

[Figure 118 on page 286](#) illustrates the *Capacity Threshold for Radio* screen.

Figure 118: Capacity Threshold for Radio

Capacity Threshold For Radio Enable Auto Refresh

Capacity Threshold For Radio													
	AP MODEL	STATION COUNT RANGE				THROUGHPUT (Mbps) RANGE				AIRTIME UTILIZATION(%) RANGE			
		IDLE	NORMAL	CAPACITY	OVERLOAD	IDLE	NORMAL	CAPACITY	OVERLOAD	IDLE	NORMAL	CAPACITY	OVERLOAD
<input type="checkbox"/>	AP1010	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP1010e	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP1014i	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP1020	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP1020e	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP110	Less than 1	1 to 6	7 to 10	More than 10	Less than 10	10 to 39	40 to 41	More than 41	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP301	Less than 1	1 to 30	31 to 40	More than 40	Less than 2	2 to 15	16 to 20	More than 20	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP302	Less than 1	1 to 30	31 to 40	More than 40	Less than 2	2 to 15	16 to 20	More than 20	Less than 20	20 to 60	61 to 75	More than 75
<input type="checkbox"/>	AP310	Less than 1	1 to 30	31 to 40	More than 40	Less than 10	10 to 80	81 to 120	More than 120	Less than 20	20 to 60	61 to 75	More than 75

3. Select an *AP Model* by clicking the check box and select the *Edit* option.
4. In the *Edit Capacity Threshold* pop-up for the selected AP Model number, modify the *Station Count Range*, *Throughput (Mbps) Range* and *Channel Utilization(%) Range* values.
5. Select *Save*.
6. The modified value for the selected AP model is displayed on the *Capacity Threshold for Radio* screen.

System Log View

The *System Log View* provides the log details of all the operations performed on NM. By default the syslog viewer displays messages from the last hour. If there are no messages in the past hour, the syslog window does not display any entries. The search for the logs can be performed in *Ascending* or *Descending* order. The system log *Date/Time*, *Application*, *Mnemonic*, *Priority*, *User*, *User Group*, and *Message* details are displayed. The *User* and *User Group* columns are displayed only if *Show All Columns* option is checked. View the *FortiWLM* logs by following these steps:

1. Navigate to *Administration > System Administration > Syslog View*. The Syslog View screen is displayed. [Figure 119 on page 287](#) illustrates the Syslog View screen.

Figure 119: Syslog View

Syslog Auto Refresh: 38 Sec

SEARCH ORDER (DATE/TIME) Descending ▾		MAXIMUM RECORDS 200 ▾		ADVANCED FILTERS...	
START TIME <input type="text"/> 		END TIME <input type="text"/> 		GET SYSLOG	
<input checked="" type="checkbox"/> NOW		<input type="checkbox"/> NOW			

Display Rows 200 ▾ 1 - 16 of 16

DATE/TIME ▾	APPLICATION ▾	MNEMONIC ▾	PRIORITY ▾	MESSAGE ▾
11/25/2013 22:36:40	NM	Administration	info	Event Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:36:39	NM	Administration	info	Alarm Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:24:34	NM	Administration	info	Event Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:24:33	NM	Administration	info	Alarm Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:24:24	security	Access	info	CLI Session opened for User upgrade from host 172.19.2.24
11/25/2013 22:24:24	security	Access	info	CLI Session closed for User upgrade
11/25/2013 22:12:20	NM	Administration	info	Alarm Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:12:20	NM	Administration	info	Event Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:00:14	NM	Administration	info	Event Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:00:13	NM	Administration	info	Alarm Re-synchronization successful for controller hostname = 172.19.2.24.
11/25/2013 22:00:06	security	Access	info	CLI Session closed for User upgrade

☐ Show All Columns

2. Modify the search order from *Ascending* to *Descending*.
3. Select the maximum number of records to display, 200, 500, 1000 or 2000.
4. Configure a *Start Time* and *End Time*.
5. Optionally, reduce the log results by adding a search filter.
 - Click *Advanced Filters > Add Filter*.
 - Select a *Filter ID*, *Operation* and *Filter Value*.
 - Click Close.
6. Click *Get Syslog*.

Export Syslog to External Server

Syslog from a FortiWLM device can be exported to an external syslog server. To export to an external server, configure the server details the type of logs to be exported.

Monitor

Configuration

Inventory

Reports & Notify

Visualization

Administration

System Administration

Server Details

Supported Controllers

Mail Servers

SNMP

Capacity Threshold

Syslog View

Syslog ?

SysLog View External SysLog

Remote SysLog* ☒ Enabled ☐ Disabled

Server IP* 10.33.115.26 Enter Server IP.

Port* 514 Default Port: 514.

NMS Emergency Select NMS Filter. (\$

System Emergency Select System Filter

Security Emergency Select Security Filter

Enter the following details:

- Select **Enable** to allow exporting the syslogs to an external syslog server.
- **Server IP**: The IP address of the external syslog server.
- **Port**: The port at which the external syslog server will accept incoming connection from FortiWLM.
- **NMS**, **System**, and **Security**: Select the type of logs from each of the category that will be sent to the external syslog server.

Syslog messages are raised during the following few scenarios:

- When a new license file is uploaded.
- When a license file is removed.
- When the APs from the maps are removed during license enforcement.
- When the controller is marked as Unlicensed/Managed in case of license violation.
- When the CA certificates are imported, exported or deleted.
- When the server certificates are imported, exported, applied or deleted.
- When you create a CSR and export the CSR requests.

See the **Syslog** screen (*Administration > System Administration > Syslog View*) in Online Help for detailed information on *Syslog View* topic.

FortiWLM Maintenance

1. Navigate to *Administration > System Administration > Maintenance*.
2. The *Maintenance* screen provides the following *Server Maintenance Parameters* to be configured.

TABLE 2. Server Maintenance Parameters

Field	Description
Server backup	
Backup Schedule	<p>The <i>Backup Schedule</i> option allows you to select a period for the backup to be performed. Select an option from the Backup Schedule list. The options are as follows:</p> <ul style="list-style-type: none">• No Schedule• Daily (default)• Weekly
Backup Day	<p>The <i>Backup Day</i> option allows you to select a day in a week for the server backup to be performed. Select any one of the following options:</p> <ul style="list-style-type: none">• Sunday• Monday• Tuesday• Wednesday• Thursday• Friday• Saturday <p>The default backup day is Sunday.</p>
Backup Hour	<p>The <i>Backup Hour</i> allows you to select a time of the day for the backup to be performed. The Time is from 1.00 A.M. to 12.00 P.M. The default backup hour is 1.00 A.M.</p>
Number of Backups To Preserve	<p>The <i>Number of Backups To Preserve</i> option allows you to enter the number of backups that can be preserved. The range varies from 1-3. The default value is 2. Enter the <i>Number Of Backups To Preserve</i>.</p>

TABLE 2. Server Maintenance Parameters

Field	Description
Transfer Backups To Remote Host	<p>The <i>Transfer Backups To Remote Host</i> option allows you to transfer the data backup to a remote host. Select an option from the <i>Transfer Backups To Remote Host</i> list. The options are as follows:</p> <ul style="list-style-type: none">• Yes - This option enables automatic transfer of server backup to remote host. By selecting this option, the following parameters related to the remote backup transfer are enabled:<ul style="list-style-type: none">• Overwrite Server Backups On Remote Host• File Transfer Protocol• Remote Host Name• User Name• Password• Remote Directory• No - This option disables the automatic transfer of server backup to a remote host and the above mentioned parameters related to the remote backup transfer.
Overwrite Server Backups On Remote Host	<p>The <i>Overwrite Server Backups On Remote Host</i> option allows you to overwrite the server backup on the remote host. Select an option from the <i>Overwrite Server Backups On Remote Host</i> list. The options are as follows:</p> <ul style="list-style-type: none">• Yes• No
File Transfer Protocol	<p>The <i>File Transfer Protocol</i> is the protocol that is used for copying the server backup to remote host. Select an option from the <i>File Transfer Protocol</i> list. The options are as follows:</p> <ul style="list-style-type: none">• FTP• SCP
Remote Host Name	Enter a name for the <i>Remote Host</i> .
User Name	Enter a <i>User Name</i> .
Password	Enter a <i>Password</i> for the User Name.
Remote Directory	Enter the name for the <i>Remote Directory</i> .

Controller Configuration Backup

TABLE 2. Server Maintenance Parameters

Field	Description
Backup Schedule	The <i>Backup Schedule</i> option allows you to enter the backup schedule. The Backup Schedule is either <i>Daily</i> or <i>Weekly</i> . Enter the <i>Backup Schedule</i> .
Backup Day	<p>The <i>Backup Day</i> option allows you to select a day in a week for the backup to be performed. Select any one of the following options:</p> <ul style="list-style-type: none">• Sunday• Monday• Tuesday• Wednesday• Thursday• Friday• Saturday <p>The default backup day is Sunday.</p>
Backup Hour	<p>The <i>Backup Hour</i> allows you to select a time of the day for the backup to be performed. The Time is from 1.00 A.M. to 12.00 P.M. The default backup hour is 1.00 A.M.</p>
Statistics	
Months to keep statistics data	<p>The <i>Months to keep statistics data</i> option allows you to set the number of months to preserve the statistics data. The statistics data older than the number of months specified in this field from the current date will be automatically deleted from the server. The statistics data includes,</p> <ul style="list-style-type: none">• Global trend• Controller trend• Controller distribution• AP dashboard• Station dashboard ->Statistics• Alarms• Syslog <p>Enter the <i>Months to keep statistics data</i>. The duration to preserve the statistics is between 1 - 6 months. The default value is 3 months.</p>

TABLE 2. Server Maintenance Parameters

Field	Description
Long term: 8 hourly data aggregation period begins at (AM)	The <i>Long term: 8 hourly data aggregation period begins at (AM)</i> option allows you to enter the start period for the data aggregation. Enter the time for the data aggregation to begin.
Statistics Polling Interval	The <i>Statistics Polling Interval</i> is the period in minutes at which the FortiWLM receives the statistics from the controller.
Discovery	
Delete unused images on controller to install agent	<p>The Delete unused images on controller to install agent option allows you to delete the unused images on the controller. Select an option from the Delete unused images on controller to install agent list. The options are as follows:</p> <ul style="list-style-type: none"> • Yes • No
Report Preference	
Number Of Records Per HTML Page For Reporting	<p>The <i>Number Of Records Per HTML Page For Reporting</i> option allows you to enter the number of records that can be displayed in the HTML Report page.</p> <p>For Example: In the <i>Number Of Records Per HTML Page For Reporting</i> field, if the number entered is 40, then only 40 records are displayed in an HTML page report. The next 40 records are printed on the next page.</p> <p>Enter the <i>Number Of Records Per HTML Page For Reporting</i>.</p>
User Interface preference section	
Attribute to be used for display controller name	<p>The <i>Attribute to be used for display controller name</i> option allows you to select the attributes to be used to display the controller name. The options are as follows:</p> <ul style="list-style-type: none"> • Hostname: The name/IP Address provided while adding a Controller (default). • Node Name: The name that is configured on the Controller.
Allow Simple Password for Local User	By default, FortiWLM requires users to follow strict password rules as part of PCI compliance. However, you can now allow users to create simple passwords by disabling this condition.

TABLE 2. Server Maintenance Parameters

Field	Description
Session Time-out in Minutes	As part of PCI compliance, unattended FortiWLM login session will timeout in 5 minutes. Select NEVER , to prevent a session being timed out.
OUI Update	
Last update time	Displays the date and time of the OUI details updated the last time.
Automatically update every week	This option when enabled, will allow the system to automatically update the OUI details every week.
Upload OUI File	This option allows you to upload the OUI file manually to update the system OUI details.

FortiWLM Diagnostics

Administration > System Administration > Diagnostics

You can collect the *FortiWLM* diagnostics comprising of NM related logs and other files, download them to a local folder and send to *Fortinet Support* to aid in troubleshooting.

1. Select *Generate Diagnostics* option on the header of the FortiWLM dashboard.
2. You will be redirected to *Administration > System Administration > Diagnostics*.
3. The data collection starts and the browser window displays the collection status and progress. After the collection is complete, a message for the successful completion of the diagnostics generation is displayed.
4. Select *OK*.
5. The downloaded file is displayed as "(Latest)" highlighted with green color.
6. In the Diagnostics screen, you can view the old and latest diagnostics with the below information and perform the following actions:

Field	Description
Date/Time	Displays the <i>date and time</i> of the diagnostics captured in mm/dd/yyyy and hh:mm:ss format.
File Name	Displays the diagnostics file name.
Size	Displays the size of the diagnostics file name in KB.

Field	Description
Download	<p>Allows you to download the diagnostics for troubleshooting. To download the diagnostics, follow the below mentioned steps:</p> <ol style="list-style-type: none"> 1. Select download icon. 2. At the <i>File Download</i> dialog prompt "<i>Do you want to open or save this file?</i>", choose one of the below mentioned options: <ul style="list-style-type: none"> • Open with: <ul style="list-style-type: none"> • Select <i>Open</i> with option to view the diagnostics. • The preferred format to view the diagnostics is <i>.tar.gz</i>. • Select <i>OK</i>. The <i>WinZip</i> application opens. • In <i>WinZip</i>, highlight the file listed in the zip archive and click <i>View</i>. The <i>View</i> dialog displays. • Save File: <ul style="list-style-type: none"> • Select <i>Save File</i> option to save the diagnostics. The preferred format to download the diagnostics is <i>.tar.gz</i>. • In the <i>Save As</i> dialog that opens, navigate to the location you wish to save the file and click <i>Save</i>.
Delete	<p>Allows you to delete the selected diagnostics.</p> <p>Select the older diagnostics by clicking the checkbox and click on <i>Delete</i> option to delete them from the Diagnostics screen.</p>

User Administration

The *User Administration* in the *Administration* allows you to configure the users and user groups and provide the access permissions.

Users and Users Group

Users can be created, grouped and assigned group privileges from the web UI of *FortiWLM*. With user groups, users are not assigned permissions directly, but only acquire them by belonging to a user group. If you do not set up controller groups, all controllers remain assigned to the controller group named *Default*. The *Default Controller group* cannot be modified by the *Super user group*. By default, *Admin* belongs to the *Super user group* and *Guest* belongs to the *Default group*. The groups *Default* and *Super user* cannot be deleted nor can their access capabilities be altered. Any member of the *Super user group* can create more user groups and add people to them. Any changes made to group privileges affect all members of the group. Configurations created by a group member can be viewed, edited, or deleted by other members of that group.

A user with administration capability and with no inventory capability can see, create/modify user groups. We do not recommend this user configuration; in most cases, you want to add the Inventory capability to *Admin* users.

User Group Access Capabilities

The *FortiWLM* access assigned to a user group determines what users in that user group can do.

- **Monitor Capability:** Access to the *Monitor* tab and its sub-tabs only - no access to any other tab. This is the default assignment for a group.
- **Configuration Capability:** Access to the Configuration tab and its sub-tabs only - no access to any other tab. To configure controllers, a user must also have Inventory Capability.
- **Inventory Capability:** Access to the Inventory tab and its sub-tabs only - no access to any other tab
- **Report and Notification Capability:** Access to the Report and Notify tabs and their sub-tabs only - no access to any other tab
- **Visualization Capability:** Access to the Visualization tab and its sub-tabs only - no access to any other tab
- **Administration Capability:** Access to the Administration tab and its sub-tabs only - no access to any other tab

Pre-existing User Groups	Administration Tab	Inventory Tab	Configuration Tab	Monitor Tab	Reports and Notification	Visualization Tab
Superuser	X	X	X	X	X	X
Default (monitor Only)				X		

Adding a User Group

To create another user group (and optionally add users immediately), follow these steps:

1. Navigate to *Administration > User Administration > Users > Add*.
2. In the *Add User Group* screen, provide a name for the user group. [Figure 120 on page 296](#) illustrates the *Add User Group* screen.

Figure 120: Add User Group

3. Optionally provide a group description.
4. Select the configuration for the user group (*Access Capability, Users, and Controller Groups*) as described below.
5. If you don't see the new group listed, click Refresh.

Access Capability	<p>Determine the group access capability by checking tabs the users will be able to click and use: <i>Administration, Inventory, Configuration, Monitor, Report and Visualization</i>. After they are all checked, click >> to move them to the right.</p> <p>A user with administration capability but no inventory capability can view, create/modify user groups. We do not recommend this user configuration; in most cases, you want to add Inventory capability to Admin users.</p>
Users	<p>Add users to the group by checking names and then clicking >> to move them to the right. (Users were created previously by clicking <i>Administration > User Administration > Users</i>.)</p>

Controller Groups	Add permission for users to access controller groups by checking controller group names and then clicking >> to move them to the right. The Default group is always present. To add more controller groups, see “Controller Group Inventory” on page 216 .
AP Groups	Add permission for users to access AP groups by checking the AP Group names and then clicking >> to move them to the right. The Default group is always present. To add more AP groups, see “AP Group Inventory” on page 219 .

6. Click Save.

The *User Groups* can be modified or deleted by selecting the user, followed by selecting the respective options.

Adding New Users

To add new users, follow these steps:

1. Navigate to *Administration > User Administration > Users > Add*.
2. In the User Accounts - Add screen, provide a *User Name* and *Password*. It is mandatory to reconfirm the password. [Figure 121 on page 297](#) illustrates the *Add User Accounts* screen.

Figure 121: User Accounts - Add

User Accounts - Add

User Name	<input type="text" value="Test1"/>	[1-31] chars., Required
Full Name	<input type="text" value="Test"/>	[0-32] chars.
Description	<input type="text" value="Testing"/>	[0-255] chars.
Email Address	<input type="text" value="abc@test.com"/>	[0-255] chars.
Contact Details	<input type="text" value="admin"/>	[0-255] chars.
Password*	<input type="password" value="....."/>	[1-32] chars., Required
Re-Confirm Password*	<input type="password"/>	[1-32] chars., Required
Group Name*	<input type="text" value="default"/> ▼	

3. Select a *Group Name*. The Group Name drop-down box includes all the names of all user groups. *Default* is listed along with any additional groups that you created. A user can only belong to one group.
4. Optionally provide *Full Name*, *Description*, *Email Address*, and *Contact Details*.
5. Click Save.

The *Users* can be modified or deleted by selecting the user, followed by selecting the respective options.

View a User's Account

To see a user's account, click *Administration > User Administration > Users > View Details*. The following details for the selected user is displayed:

- User Name
- Full Name
- Description
- Email Address
- Contact Details
- Password (*****)
- Group Name
- Last Updated

See the ***Users and User Groups*** screens (*Administration > User Administration > User Groups and Users*) in Online Help for detailed information on *User Groups and Users* topic.

Remote Administrators

You can add users who can authenticate via TACACS or RADIUS server to access FortiWLM servers. To add a user with TACACS login, do the following:

1. In the FortiWLM WebUI, Go to **Administration > User Management** page.
2. Select the authentication type as TACACS+ and enter the following details about the TACACS server:

User Management - Update

Authentication Type: ☐ Radius ☒ Tacacs+ ☐ Local

Primary TACACS+ IP Address	<input type="text" value="0.0.0.0"/>	
Primary TACACS+ Port	<input type="text" value="49"/>	Valid range: [0-65535]
Primary TACACS+ Secret Key	<input type="text"/>	
Secondary TACACS+ IP Address	<input type="text" value="0.0.0.0"/>	
Secondary TACACS+ Port	<input type="text" value="49"/>	Valid range: [0-65535]
Secondary TACACS+ Secret Key	<input type="text"/>	

Enter the second TACACS server details for resiliency.

To add a user with RADIUS login, do the following:

1. In the FortiWLM WebUI, Go to **Administration > User Management** page.
2. Select the authentication type as RADIUS and enter the following details about the TACACS server

Authentication Type ☒ Radius ☐ TACACS+ ☐ Local

Primary RADIUS IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Primary RADIUS Port	<input type="text" value="1812"/>
Primary RADIUS Secret Key	<input type="text"/>
Secondary RADIUS IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Secondary RADIUS Port	<input type="text" value="1812"/>
Secondary RADIUS Secret Key	<input type="text"/>

FortiWLM Licensing

The Licensing infrastructure is within *FortiWLM* and is applicable to the entire services appliance. The *FortiWLM* implements the license enforcement based on the AP count.

The *License* screen allows you to import a feature license key file for *NM* and its features installed on services appliance. You can request for *NM* license and upload it using *NM* web UI. A separate license key file is required for each feature that requires a license for operation. For instructions on procuring the license key file, see the [“Add a License” on page 35](#). Only one file can be selected and uploaded at a time. The Licensing Manager resumes whenever E(z)RF server restarts after a shutdown.

License Recovery and Backup

Licenses are a part of the server backup.

Licensing and Upgrade

The licensing is applicable after server reboots post the upgrade process. It is recommended to upload the license files before the upgrade. If licenses are not available after upgrade, APs will be marked unlicensed and the server is switched to a time limited validity. License (FortiWLM-NM-BASE) is required to monitor and manage controllers through *FortiWLM*. The License must be upgraded before it expires. The license expiry alarm is raised by the *FortiWLM* 30 days before its expiry. The License Violation message is displayed in the following scenarios:

- When the number of APs exceeds the number of licenses available for EZRF-NM-BASE feature.

- When the license for EZRF-NM-BASE feature has expired.

A grace period of 30 days is provided, during which the system functions normally. After the grace period, the controllers which does not have the required number of licenses for APs are marked as *Unlicensed* and will not be monitored by the *FortiWLM*. After licenses are added, the unlicensed controllers are automatically monitored by the Network Manger.

To access the Licensing through the NM web UI, perform the following steps:

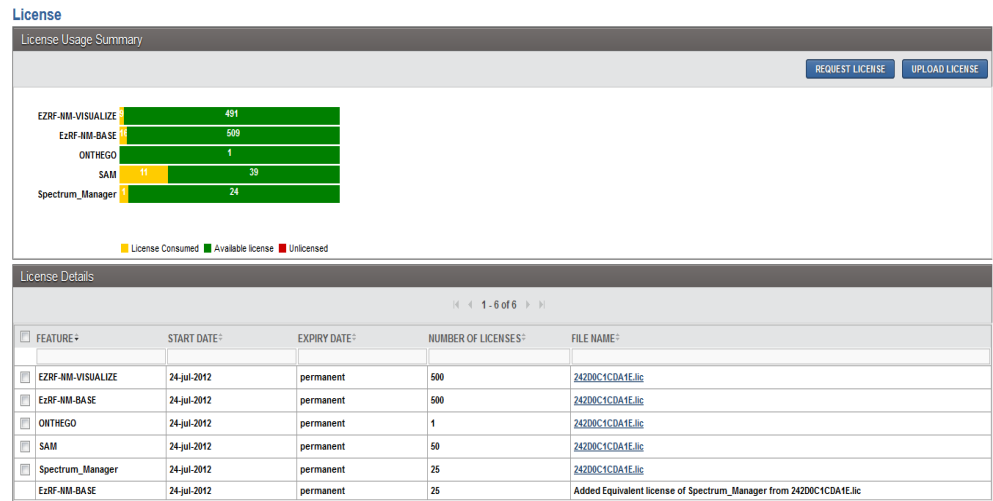
1. Navigate to *Administration > User Administration > License*. See [Figure on page 300](#).
2. The *License* screen displays two sections as follows:
 - “*License Usage Summary*” on page 300
 - “*License Details*” on page 301

License Usage Summary

The *License Usage Summary* section provides a graphical representation of the License usage for *EZRF-NM-VISUALIZE*, *EzRF-NM-BASE*, *SAM* and *Spectrum Manager*. The following graphs provide the visual representation of license usage. [Figure 122 on page 300](#) illustrates the *License Usage Summary* screen.

- **License Consumed** - The number of used licenses is represented in YELLOW color.
- **Available licenses** - The number of unused licenses is represented in GREEN color.
- **Unlicensed** - The number of unlicensed licenses is represented in RED color.

Figure 122: License Usage Summary



The *License Usage Summary* section also provides the following links:

Request License

- Select *Request License* link to view the complete information of the license. The license information provides the following details:
 - **Serial Number** - Displays the manufacturer serial number.
 - **License Entitlement/Certificate ID** - Displays the License Entitlement number or the Certificate ID.
 - **System ID** - Displays the ID of the System.



The System ID is displayed only for SA200 and SA2000 services appliance.

-
- **VENDOR_STRING** - Displays the 32 digit hexadecimal ID of the system.



The VENDOR_STRING is displayed only for the SA2000-VE platform.

-
- **Feature Name** - Displays the name of the feature (*EZRF-NM-BASE, SAM and Spectrum_Manager, and so on*) being licensed.
 - **Number of licenses** - Displays the total number of licenses issued.
 - **License Duration** - Displays the duration of the license (Permanent or Trial).
 - Click the **Select All** button, to copy the above mentioned information and click **Close**.

Upload License

- Select *Upload License* Link.
- In the *Upload License* file screen, click *Browse / Choose* file button to locate and upload the license file (.lic).



The *Upload License* allows a single license file upload. It does not provide the ability to upload multiple license files in one upload operation/session.

License Details

The *License Details* section summarizes the total number of licenses and provides the complete information about each of them. It provides the details of the *Feature, Start Date, Expiry Date, Number Of Licenses* and *File Name*.

See the **License** screen (*Administration > User Administration > License*) in Online Help for detailed information on *License* topic.



It may take 1-10 minutes to reflect the licenses after the license file is uploaded.

Limitations: The path of the license file saved, must not be too long. The license cannot be applied during such scenarios.

Backup Administration

The *FortiWLM* server provides an option to backup and restore the database. The backup database is stored on the server in a pre-defined location. The administrator can restore the database from the backup files. The data backup requires 5GB of free disk space which includes the following information:

- Maps
- Reports
- Licenses
- Controller configuration backup files
- Upgrade logs
- **Database Information:** The database information includes the **nmsdb** database and **eventdb** database.

The backups have two different naming conventions that is, one for a complete backup and the other is for the configuration-only backup. The backups are stored in tar file format.

Automated Backup

The data backups can be scheduled daily or weekly. The following are the default values:

- The daily backups are scheduled by default at 1.00 a.m.
- The weekly backups are scheduled by default at 1.00 a.m. on Sunday.

See "*FortiWLM Maintenance*" on **page 289** for further details.

Backup History

The *FortiWLM* backup history can be viewed by following the below mentioned steps:

1. Click *Administration > Backup Administration > Backup History*.
2. The *Backup History* screen is displayed providing the log of the backup and restore activity.

The two possible states for a backup are *Passed* or *Failed*.

If a backup or restore fails, an alarm is raised displaying an error message which is logged into the file `/data/apps/nms/logs/backup_restore.log`. An alarm is raised only if the backup fails.

To accomplish this from the CLI, use the command **sh backup**; this command lists all backup entries in the backup **directory** `/data/backup/nms`.

If a backup failed after reaching the maximum hard disk size, the backup entry is listed in the backup history table as **failed**. Also, a failure message is stored in the **log backup_restore.log**. To view the **backup_restore.log**, use the CLI command **show backup-restore-history**. This lists the last 25 entries in the log.

Restoring a Backup

You can restore a backup only from the command line interface (CLI). The following are lists of commands to restore a backup:

- **sh backup** lists all backup entries (including failures) in the backup **directory** `/data/backup/nms`.
- **show backup-restore-history** displays the last 25 backup entries and all failure messages in the **backup_restore.log**.
- **restore <filename>** restores the complete backup.
- **backup [config-only]** performs a backup configuration data.
- **backup [all]** performs a backup complete server data.

See the [“Appendix E - Command Line Interface” on page 493](#) command for details.

Restoring a Backup From External Location

The backups are stored in the tar file.

To restore a backup from an external location, use the **copy** command to *copy* the file back to the appliance, and then use the **restore** command to *restore* the backup. You can also use the CLI command **show backup-restore history** to see all saved backups.

Two backups from the command **backup all** are saved by default. The results of **backup config-only** are not automatically deleted. All of those tar files are saved until you delete them.

An admin can recover a backup from the CLI with the command **restore**. You have two restore options, either *restore the entire backup* or *restore only the configuration information*.

For example, to restore the entire backup *Backup-2014-03-05*, including statistics, from the backup **directory** `/data/backup/nms`, use this command:

```
default# restore Backup-2014-03-05-01-01-01.tar.gz
```

Restoring only the configuration information restores information like *maps*, *controller details*, and *AP details*. Other than statistics, everything is restored.

For example, to restore the configuration only from the file Backup-2014-03-05, use this command:

```
default# restore Backup-2014-03-05-01-01-01.tar.gz config-only
```

Restoring a particular table in the database is not supported.



Restoring the backup data depends upon the data present in the server.

Deleting a Backup

You can delete a backup only from the command line interface (CLI). The following are list of commands to delete a backup:

- **sh backup** lists all backup entries (including failures) in the backup **directory /data/backup/nms**.
- **show backup-restore-history** displays the last 25 backup entries and all failure messages in the **backup_restore.log**.
- **delete backup** deletes backups.

See the [“Appendix E - Command Line Interface” on page 493](#) command for details.

For example, the command **delete Backup-2014-03-05-01-01-01.tar.gz** deletes the backup named **Backup-2014-03-05-01-01-01.tar.gz** from the backup **directory /data/backup/nms**

Preserve Backup on Remote Server

To preserve backup on remote server you must transfer the data backup to a remote host. Refer to the [“Transfer Backups To Remote Host” on page 290](#) for further information.

Cleaning up of unwanted data

The server automatically deletes the historical statistics of backup. Configure the *“Number of Backups To Preserve”* on **page 289** and the number of *“Months to keep statistics data”* on **page 291** to reduce the disk usage.



A minimum of 5GB free disk space is required to backup the data.

If you want to preserve backups before they are deleted, copy them from the appliance to another location with the CLI copy command, for example:

```
#copy /data/backup/nms/Backup-2014-03-05-01-01-01.tar.gz ftp://anonymous@<ip address>/
```



Ensure to copy the latest backup file off the box periodically.

Use the CLI commands **backup all** or **backup config-only** to perform a CLI backup of the appliance when you are logged in as admin; When you execute these CLI commands, the web UI history is also updated.

Flash Backup and Restore with Snapshot

The services appliance comprises of a partitioned flash. Two copies of the flash image are maintained so that you can restore the flash if the original becomes corrupted. The flash recovery feature verifies existence of at least one snapshot of the disk on every Saturday and automatically creates a snapshot of the boot partition on the disk, if there is no partition. This ensures that there is at least one snapshot of the disk, though you may not have created it yourself.

The snapshot CLI commands let you copy, view, and delete the flash configuration on the hard disk in the services appliance. For command details see See the *“Appendix E - Command Line Interface”* on **page 493** command for *snapshot create*, *snapshot delete*, *snapshot restore*, and *show snapshot* command details.

Create a Flash Backup on Disk with Snapshot

To create a snapshot of the flash configuration on the hard disk of the services appliance, use the command **snapshot create**:

```
default# snapshot create
```

You booted from the primary partition

This command will create an exact copy of the mirror partition which will be synchronized with the primary partition before the snapshot is created. During the snapshot, services will continue to run, but you will not be able to run other commands on this console and system performance will be impacted. We recommend that you use this command during off-peak hours.

Do you want to proceed? [y/n] y

Syncing disks... done

Copying Data: #####

Operation completed successfully

To view the snapshot, use the command **show snapshot**:

Snapshot files are archived under - **/data/backup/snapshot/**

Use the **copy scp** option of the CLI command to move this file off the machine.

```
default # show snapshot
```

```
snapshot.2.1-29.23:44-10-12-2014
```

```
default#
```

You can delete the snapshot.

```
default# snapshot delete snapshot.2.1-29.23:44-10-12-2014
```

```
snapshot.2.1-29.23:44-10-12-2014 deleted
```

Limitations for Flash Backup

If you cancel a snapshot backup midway, the incomplete backup is not listed with an error the way a complete backup with an error is listed. Delete an interrupted incomplete backup immediately so that no one tries to restore it.

Restore a Snapshot

Use a snapshot to restore a (possibly corrupted) flash partition.

The command **snapshot restore** reconfigures a services appliance to use the snapshot version of flash. The restore command copies a selected snapshot image back to the backup partition. Synchronization does not start until after rebooting in order to avoid tainting the newly

restored partition. Therefore, a second reboot is required. When the next reboot takes place, the system should be rebooted from the restored partition and the original partition will then be updated to match the newly restored partition. The system can then be run from either partition, since they are again identical.

A snapshot will always be restored to the backup partition. If you booted to the primary partition (hda2), then the image will be restored to the mirror partition (hda3). Alternatively, if you booted to the mirror, the image will overwrite the primary. The mirror/primary are equivalent from the system standpoint. They are only named this way because GRUB will automatically boot to the primary partition without manual intervention.



After restoring the snapshot, reboot the system to boot from the primary partition.

Snapshot Restore Example

```
default# snapshot restore snapshot.16:00-04-05-2014
```

You booted from the primary partition.

This command will copy the snapshot image snapshot.16:00-04-05-2014 to the mirror partition.

During snapshot, services will continue to run, but you will not be able to run other commands on this console and system performance will be reduced.

It is recommended to run this command during off-peak hours.

Do you want to proceed? [y/n] y

Copying Data: #####

Operation completed successfully.

Reboot the system now and select the mirror partition following the directions [“Reboot a Services Appliance and Select a Partition” on page 308](#). The services appliance will be restored to the snapshot version of flash (both primary and secondary).

Corrupted Flash Example

Use the snapshot to recover when a corrupted flash boots with a message like this:

```
Booting 'BOOT FROM PRIMARY IMAGE'
```

```
root (hd0,1)
```

```
Filesystem type unknown, partition type 0x83
```

```
kernel=/boot/vmlinuz root=/dev/hdc2 console=tty0 console=ttyS0,115200  
crashkern
```

```
el=64M@16M rhgb quiet
```

```
Error 17: Cannot mount selected partition
```

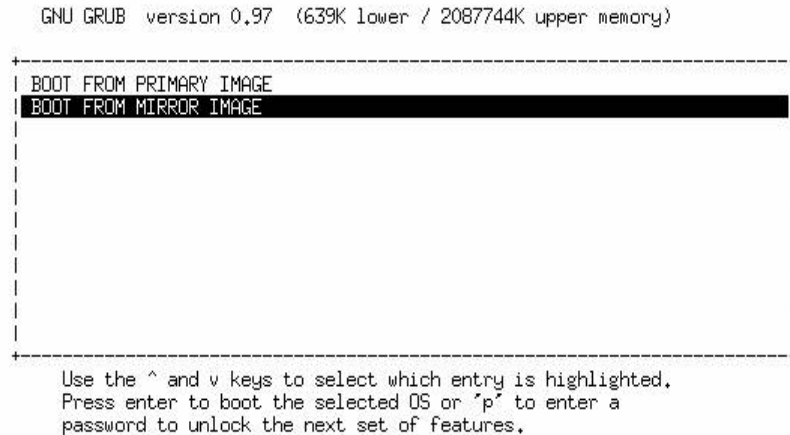
```
Press any key to continue...
```

Reboot a Services Appliance and Select a Partition

The services appliance boots by default from primary flash, but can be configured to boot from mirror flash. To change the boot flash partition, follow these steps:

1. Reboot the services appliance. During reboot, you see the question in [Figure 123 on page 308](#).
2. Immediately press Enter to stop the boot process.
3. Select one of the options in [“Flash boot change” on page 308](#) and press Enter.

Figure 123: Flash boot change



4. Booting continues with one of the following messages - the pertinent text for SA200 is highlighted in blue below.

```
Booting 'BOOT FROM PRIMARY IMAGE'
```

```
Root (hd0.1)
```

```
Filesystem type is extfs, partition type 0x83
```



```
kernal=/boot/vmlinuz root=/dev/hdc2 console=tty0 console=ttyS0, 115200  
crashkernel=64M016M
```

```
[Linux-bzImage, setup=0x1400, size=0x25ddc0]
```

-----OR-----

Booting 'BOOT FROM MIRROR IMAGE'

Root (hd0.2)

Filesystem type is extfs, partition type 0x83

```
kernal=/boot/vmlinuz root=/dev/hdc2 console=tty0 console=ttyS0, 115200  
crashkernel=64M016M
```

```
[Linux-bzImage, setup=0x1400, size=0x25ddc0]
```

Copying Data: #####

Operation completed successfully

With SA200, if you see hdc2 as the backup partition, then you are running from the mirror partition (hdc3). With SA2000, it is the opposite - if you see hdc3 as the backup partitions, then you are running from the mirror partition.

Storage

The *FortiWLM* handles multiple system activity like *Event Log*, *Alarm History*, *Station Activity Logs*, *User activity Log (Sys Log)*, *NM backups*, *SD backups saved on the NM server*, *Statistics data*, *Inventory and configuration data*, and *E(z)RF system data*. All the above mentioned system activities are stored in the database files which occupy enormous space. The Storage in the *Administration* allows you to archive all the above mentioned data based on polices.

Station Activity Log

The *NM* is designed in such a manner that each system activity mentioned above is managed in a clever way occupying space. Although, *NM* performs periodical backup and deletes the data from the database, different other configurations are performed, where the operations are executed on the activity data storage. Following are some of the activities:

- Query and view data from the *NM* web UI
- Modify data
- Export data into file from the *NM* web UI

- Backup activities including one time backup and scheduled backup
- Purge activities including one time purge and scheduled purge
- Forward activity records to the external system, user side SNMP manager or email or others.
- Monitor the storage: disk space / number of records / date and time of records

The above mentioned operations are archived in the database. The current design of *NM* database comprises of **nmsdb** and **eventdb** database partitions. The disk monitoring and station activity log archival is performed on the *eventdb* partition of the *NM* database.

The above mentioned operations on *NM* are archived through the *NM* web UI.

1. Select *Administration > Storage > Station Activity Log*. The *Station Activity Log Archival Policy* screen is displayed. The station events here are archived based on the following policies:
 - **Events Archival Policy:** The events are archived in a compressed format and then deleted from the NMS.
 - **Events Retirement Policy:** The events are archived based on the retirement age or maximum disk space.
2. The *Station Activity Log Archival Policy* screen consists of the following three sections:
 - **Disk Usage:** The *Disk Usage* is a pie chart that displays the total Available space and the Used space utilization by the events. The disk usage of 30 GB is provided for the SA200/SA250 and the disk usage of 60 GB is provided for SA2000.
 - **Station Activity Log History:** The *Station Activity Log History* graph displays the disk space utilization by the events as bar chart. The "X-Axis" depicts the Day in mm-dd-yy format and "Y-Axis" depicts the Disk Usage in GB.
 - **Storage Configuration:** The *Storage Configuration* is based on the Station Activity Log Retirement Policy which enforces the events archival or deletion based on the disk space usage. A maximum of 30 days station log activity events are displayed on the graph. The Storage configuration provides the following options:
 - **Amount of storage to free in retirement:** The *Amount of storage to free in retirement* displays the amount of storage to be deleted during retirement. This is the default selection, where 20% of the events get archived or deleted when the disk usage reaches 100% of 30 GB in SA200/SA250 and 100% of 60 GB in SA2000.
 - **Enable auto system retirement:** The *Enable auto system retirement* option enables the automatic retirement when SA200/SA250 reaches 100% of 30 GB and SA2000 reaches 100% of 60 GB.
 - **Log Retire Options:**
 - **Purge:** This option allows you to delete the records following a configurable pre-defined setting. The Station activity log purge is based on the percentage of disk usage.

- **Archive to remote server & Purge from NMS Server:** This option exports the Events in CSV format and transfers the events to a remote server using ftp/scp protocol and then gets deleted from the NMS. Once all the event tables from oldest events first are selected and exported, the directory will be compressed in tar.gz format. The compressed file is named in backup_events_dd-mm-yy-mm-hh-ss.tar.gz format. The file is then transferred to remote server using the *ftp* and *scp*. The compressed file located on the local hard drive gets deleted after the transfer.

Security Administration

The *FortiWLM* provides infrastructure to manage SSL certificates for various server applications that requires SSL certificate based authorization. The key services are:

- **WEB Server Application or Security Certificate** (See [“Security Certificate” on page 311](#))
- **VPN Server Application or VPN Administration** (See [“Configuring VPN Connections” on page 313](#))

Security Certificate

Certificates provide security assurance validated by a *Certificate Authority* (CA). This chapter describes the process to obtain and use certificates. For a Custom Certificate to work properly, you must import not only the Server Certificate, but the entire chain of trust starting with the issuer certificate all the way up to the Root CA. Server certificates are generated based on a specific *Certificate Signing Request* (CSR) and, along with the server certificate, you should get the entire chain of trust.

Generate CSR on the FortiWLM

The Certificate Signing Request or the CSR is a request sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Generate a Certificate Signing Requests (CSR) directly on the *NM* using the web UI by following the below mentioned steps:

1. Select *Administration > Security Administration > Certificate Management*. The *Certificate Management* screen is displayed.
2. The *Certificate Management* screen displays the following tabs:
 - [“Server Certificates” on page 311](#)
 - [“Trusted Root CA Certificates” on page 312](#)

Server Certificates

The server certificates provides a list of generated Certificate Signing Request (CSR) and server signed Certificates.

1. In the *Server Certificates* tab, click *Create CSR*.

2. In the *Create CSR* window, provide the Certificate Alias, Common Name and Email Address
3. Optionally provide the Organizational Unit Name, Organization Name, Locality Name, State or Province Name and Country Code
4. Click Apply. The CSR is generated and appears on the *Server Certificates* tab Click *Close*.
5. Send the CSR to the Certificate issuer for it to be processed. If the CA asks for the operating system type, select Open SSL (if available) or Other.
6. The Certificate entry now displays in the *Server Certificates* page under "Pending CSR." This entry will be matched to the certificates when they arrive and imported, ensuring that the controller that requested certificates is the only one to use those certificates.



Only the certificates with the *Status type CSR Generated* can be exported to *Export CSR* and can be saved to the hard disk. The other Status types like *In Use*, *Available*, and *Apply Failed*, cannot be exported and saved on to the hard disk.

Import the Certificate

Remember that certificate request is sent to a CA for authorization. The issued certificate is then stored in an appropriate location. You can either use your own certificates or download factory-issued certificates from Fortinet.

1. Navigate to *Administration > Security Administration > Certificate Management > Server Certificates tab > Import*.
2. In the *Import Certificate* wizard, browse for the authorized *Certificate File* by selecting the *Browse* option. Select the *Certificate Alias* name that is to be imported from the drop-down list. Select *Save*. The authorized certificate is now imported.



Before applying the certificate, ensure if the corresponding CA is located under the trusted root repository by verifying the certificate's validity and the expiry date.

3. Other actions like *View CSR*, *Export*, and *Delete* can be performed.

Trusted Root CA Certificates

The *Trusted Root CA Certificates* screen displays a list of trusted third party certificates. Any client or server software that supports the certificates maintains a collection of trusted CA certificates. These CA certificates allows *NM* to validate other certificates. *NM* can validate only certificates issued by one of the CAs in its Trusted Certificates Repository.

Import the Certificate

1. Navigate to *Administration > Security Administration > Certificate Management > Trusted Root CA Certificates tab > Import*.

2. In the *Import Certificate* wizard, browse for the authorized *Certificate File* by selecting the *Browse* option. Select the *Certificate Alias* name that is to be imported from the drop-down list. Select *Save*. The authorized certificate is now imported.



Before the certificate is applied to an application, a basic verification is performed to ensure,

- if the certificate is a valid x.509 standard certificate,
- if the expiry date has not crossed, and
- if the imported certificate is actually a Root CA certificate.

-
3. Other actions like *Export CSR* and *Delete CSR* can be performed.

See the **Certificate Management** screen (*Administration > Security Administration > Certificate Management*) in the Online Help for detailed information on *Certificate Management* topic.

Configuring VPN Connections

The virtual private network or the VPN based secure communication is enabled between the controller and *FortiWLM*. Only those controllers that are listed in the *FortiWLM's VPN controllers and status list* are allowed to setup a VPN Tunnel with the *FortiWLM* server. Both VPN Controllers and non-VPN Controllers are managed at the same time with each controller being configurable to VPN and is set to the VPN tunnel with *NM*. The tunnel with the VPN server must be established prior to other communications by the *NM*. While using VPN, the controller and *NM* server consists of the tunnel IP address within the *NM* tunnel subnet. This tunnel IP-address is used by all applications and processes within the VPN Node (*Controller, FortiWLM, SAM, and Spectrum Manager*) to communicate with other nodes. For VPN based communication, the endpoint of the tunnel serves as the *NM* server address.

Configuring the VPN

The system administrator must first configure the VPN connection settings on the services appliance. To configure VPN:

1. Select *Administration > Security Administration > VPN Administration*.
2. Select the *VPN Server* tab. Enter the desired configuration for the VPN server. Provide the *VPN Service, Encryption, VPN Server Port, IP Pool* and *Net mask* details.



To reflect the changes performed on the *VPN Server* screen, the VPN service must be restarted. The restart is performed automatically.

-
3. Click *OK* to save the changes. The services appliance is now configured for VPN service and the details are displayed on the *VPN Controllers and Status* screen.

View the VPN Controllers and Status

The VPN Authorized Clients and Status screen displays a list of clients that are added. It displays the IP Address, VPN Tunnel IP Address, VPN Authentication Status and VPN Connectivity Status of each

See the **VPN Administration** screen (*Administration > Security Administration > VPN Administration*) in the Online Help for detailed information on *VPN Administration* topic.

High Availability

High availability provides concurrent and persistent server access using a cluster two instances (primary and backup) of Network Manager. After setting up HA, the Network Manager Server is accessed via a virtual IP. When the connection to the primary server is lost, the backup server continues to provide all services. After the primary server recovers, the control is transferred to the primary server. New data collected by the backup server (during primary outage) is copied and synced between both primary and backup servers.

Configuring High Availability

Configuring HA requires you to add settings to both the servers (primary and backup). To begin setting up HA, access the WebUI of one of the server instance that should be configured as the primary server.

Setting up Primary Server

Go to **Administration > High Availability > Cluster Configuration** and update the following:

- Server Mode: Since this server is to be configured as the primary server, select **Primary Server**.
- Secondary Server: Enter the backup server IP address.
- Enter the Shared Secret key.

Click the **Save** button to enable HA functionality.

New tabs **HA Authentication**, **IP Address High Availability** and **Status** are enabled after you save the settings.

HA Authentication (Primary Server)

This tab provides options to export the SSH authentication file which is later imported in the backup server and import the exported SSH authentication file from the backup server.

Click on **EXPORT AUTHENTICATION** to export the SSH authentication file to the local machine, to be later imported into the backup server.

Click on **IMPORT AUTHENTICATION** to import the SSH authentication file which is exported from the backup server.

IP Address High Availability (Primary Server)

This tab provides options to configure the virtual IP address for HA access.

1. Enable VRRP.
2. Set the **Server Mode** as **Master**.
3. Enter the Virtual IP Address. This address must be from the same subnet and DHCP pool use to provide the IP address of both instances of the FortiWLM servers. It is recommended that you use a static IP as the virtual IP.
4. Ethernet Interface is automatically populated based on the model of FortiWLM Servers.
5. Enter a **Shared Secret key**. This key is used by the server to maintain keep alive between the two servers.

Setting up the Backup Server

In the WebUI of the backup server, update the following:

1. Server Mode: Since this server is to be configured as the backup server, select Backup Server.
2. Enter the IP address and Hostname of the Primary Server.
3. Enter the Shared Secret key.
4. Click the Save button.

New tabs, **HA Authentication** and **IP Address High Availability** are enabled only after you save the settings.

HA Authentication (Backup Server)

This tab provides options to export the SSH authentication file which is later imported in the primary server and import the exported SSH authentication file from the Primary server.

Click on **EXPORT AUTHENTICATION** to export the SSH authentication file to the local machine to be later imported to the primary server.

Click on **IMPORT AUTHENTICATION** to import the SSH authentication file which is exported from the primary server.

IP Address High Availability (Backup Server)

This tab provides options to configure the virtual IP address for HA access.

1. Enable VRRP.
2. Set the **Server Mode** as **Master**.

3. Enter the Virtual IP Address. This address must be from the same subnet and DHCP pool use to provide the IP address of both instances of the Network Manager servers. It is recommended that you use a static IP as the virtual IP.
4. Ethernet Interface is automatically populated based on the model of Network Manager Servers.
5. Enter a **Shared Secret key**. This key is used by the server to maintain keep alive between the two servers.

Status

Replication Status shows the available servers in the cluster. The cluster table contains status of the servers whether they are presently up or not and also shows the configured status of the server.

If one server is down it shows the status as "Not working". The configured server could be either Backup Server or Primary Server. User can identify the server status by logging into the server and checking the server status and for the logged in server it shows as "this server". Also users can check the configured IP addresses of the both Master and Backup node.

Disabling the HA Cluster

You can disable the HA Cluster and make the primary and backup servers run independently. Perform the following steps on the primary and backup servers.

1. Go to **Administration > High Availability > Cluster Configuration**.
2. In the **Setup** tab, set the **Server Mode** to **Disabled**.
3. Click the **Save** button to disable the HA cluster.

High Availability ⓘ

CLUSTER CONFIGURATION

Setup
 HA Authentication
 IP Address High Availability
 Status

FortiWLM Supports two node cluster. Each node is fully active and at any given time only one node can receive and respond to request in the cluster.

Disabled - Cluster support is disabled.
 Primary Server - In the cluster one and only one node should be enabled as Primary Server. The other node contact the Primary Server during the initial setup.
 Backup Server - Each other server should be setup as a Backup server.

Once initial setup has taken place all servers behave identically.

Server Mode:

☒ Disabled
 ☐ Primary Server
 ☐ Backup Server

Primary Server

(IP Address)
(Hostname)

Shared Secret:

(Leave blank to keep existing shared secret)

The Shared Secret should be the same on all servers in the cluster. It is used to authenticate servers to each other.

SAVE

Note:

- Reboot the backup node after disabling the HA cluster.
- By default, services on the backup node do not restart after the cluster is disabled. This is because the Controllers start the discovery process on both the primary and backup Forti-WLMS. To restart and use the backup node independently, contact the Forticare Support.
- Once services are restarted on the backup node, delete the existing Controllers and start managing with the new set of Controllers.

9 Service Assurance Manager

Service Assurance Manager (SAM) is a predictive diagnostic software with trouble-prevention capability. It diagnosis the health of the wireless network and reports the issue before the users are impacted. The *FortiWLM* infrastructure is used to perform end-to-end system tests, either on-demand or automatically at pre-configured intervals. End-to-end performance tests are run by activating a Virtual Client (VAP) on Fortinet Access Points. Network baseline tests are created and tests are run in the background while *SAM* is still servicing wireless clients. Once baseline network performance is established, any tests that deviate from the baseline can trigger automatic notification. Multiple tests can be configured with *SAM*. Proactive tests are as follows:

- Connectivity tests to measure packet loss and latency
- Voice tests to measure voice quality
- Throughput tests to measure performance

The tests can be configured to run on a variety of wireless profiles like clear, WPA2PSK, and WPA2-AES for every *ESS Profile* available in the *WLAN*. *SAM* summarizes the results obtained and automatically mails to pre-configured destinations.

10 Configuring SAM

Baseline Testing

A baseline, like the name implies, is a standard for future comparison. Baselines are established in *SAM* by running a virtual client to all APs on a controller and measuring the results. This baseline is used for future *Scheduled Test* comparisons at regular intervals.

Design a Baseline

When you design a baseline, the number of controllers sharing an ethernet port connection and bandwidth is taken into consideration. Performing concurrent tests on multiple controllers sharing bandwidth affects testing thresholds set in the baseline. The controller's thresholds are programmed based on the number of controllers. For an accurate comparison, the bandwidth must be the same for subsequent comparisons against the baseline. Another way to alter baseline thresholds is to remove APs and/or SSIDs from the test.

The design of a baseline does not affect throughput, latency or packet loss. The *throughput*, *latency*, and *packet loss* during a baseline connectivity test depends on the environment (number of packets in the air) when a virtual client is operating. However, the number of APs present while configuring a baseline does not affect the results.



Bridged traffic is not displayed in the throughput, as it does not pass through the controller.

Add a Baseline

We have two options to execute the baseline tests.

- **Configured Test:** This option allows you to create a baseline test by providing theoretical values.
- **Measured Test:** This option allows you to create a baseline test by providing the actual baseline values. It is important to run a measured baseline when the wireless network is operating either normally or under optimal conditions, as it is used to evaluate subsequent tests. To create either type of baseline, follow these steps:

1. Navigate to *Configure > Tests > Baseline Tests > Add Baseline*.

Figure 124 on page 324 illustrates the *Add Baseline Test* screen.

Figure 124: *Baseline Test - Add*

Baseline Tests

Baseline Test - Add

Name*

Doc

(1 - 31 chars max)

Controller Name*

172.18.60.14

Test Type

Connectivity

Notification

None

Notification Message

(max 64 chars)

Retries*

2

(0-2)

Redo Failed Tests*

☒

Signal Strength Check

On

Logging Detail

Log only critical messages

Controller IP*

172.18.60.14

Baseline Type

Measured

Notification Profile

SAM4dot0

Timeout*

30

(10-30 Sec)

Tunnel Type

Ether IP

Signal Strength Threshold*

-70

(-85 to -30 dbm)

Good Signal

Poor Signal

No Signal

No Neighbor

IF ID | ESS Profile

☐ Drav-bug39590

☐ AP-5-1

☐ AP-5-2

Select All

Clear All

Include

Exclude

Save & Run

Cancel

2. In the *Baseline Test - Add* screen, provide the following required information:

Field	Descriptions
Name	Provide a name of the <i>Baseline Test</i> primarily for usage. The name consists of up to 31 characters, including numbers, letters, capital letters, and special characters. Special characters cannot be used
Controller Name	Select the <i>Controller Name</i> or the Host name from the drop-down list. The controller name displayed, is the controller mapped to the <i>FortiWLM</i> inventory; the baseline runs on the indicated controller.
Controller IP	Select the <i>Controller IP</i> address from the drop-down list. The controller IP address displayed is the controller mapped to the <i>FortiWLM</i> inventory; the baseline runs on the indicated controller.

Field	Descriptions
Test Type	<p>Select the <i>Test Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> Connectivity: <i>Connectivity</i> describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another. The selection of the <i>Test Type</i> as <i>Connectivity</i> determines the rest of the options on the page. Refer to “Test Type - Connectivity” on page 326. Throughput: <i>Throughput</i> is the amount of data moved successfully from one place to another in a given time period. The selection of the <i>Test Type</i> as <i>Throughput</i> determines the rest of the options on the page. The throughput test type can further be divided as follows: <ul style="list-style-type: none"> Throughput TCP (Transmission Control Protocol) Refer to “Throughput - TCP” on page 327 Throughput UDP (User Datagram Protocol) Refer to “Throughput - UDP” on page 327 Voice: <i>Voice</i> is simulated using multiple thread of ping traffic. The selection of the <i>Test Type</i> as <i>Voice</i> determines the rest of the options on the page. Refer to “Test Type - Voice” on page 329. <p>The scheduled tests that run on the selected controller must match the test type in order to measure against the baseline.</p>

Field	Descriptions
Test Type - Connectivity	
By selecting the <i>Test Type</i> as <i>Connectivity</i> , the following fields appear:	
Baseline Type	<p>Select the <i>Baseline Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> Configured: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields: <ul style="list-style-type: none"> Latency (Connectivity test only): Latency is an expression of how much time is taken for a packet of data to get from one designated point to another. A low latency network connection generally experiences small delay times, while a high latency connection generally suffers from long delays. Provide a latency value for a baseline connectivity test (1-1000ms). The default value is 100. Packet Loss % (Connectivity test only): Packet loss is the failure of one or more transmitted packets to arrive at their destination. Enter the packet loss % value. The default is 0. Measured: The measured option allows you to run the baseline test. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (<i>Connectivity</i>, <i>Throughput</i> or <i>Voice</i>) will take precedence over this test. This option enables the following fields: <ul style="list-style-type: none"> Notification: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list. Notification Profile: Select the notification profile from the drop-down list. The notification profiles are configured in the FortiWLM. (<i>FortiWLM > Reports & Notify > User Preference > Notification Profiles</i>). Notification Message: Type a notification message (max 64 chars). <p>The “Advanced Options” on page 330 are displayed when the <i>Baseline Type</i>, <i>Measured</i> is selected.</p>

Field	Descriptions
Throughput - TCP	
Baseline Type	<p>Select the <i>Baseline Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Configured: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields: <ul style="list-style-type: none"> • Throughput: Enter the <i>Throughput</i> value (1-150 Mbps). • Stream: Select the <i>Stream</i> from the drop-down list. The options is Up (default), Down. • Measured: The Measured option allows you to run the baseline test. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (<i>Connectivity, Throughput or Voice</i>) will take precedence over this test. This option enables the following fields: <ul style="list-style-type: none"> • Notification: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list. • Notification Profile: Select the notification profile from the drop-down list. The notification profiles are configured in the <i>FortiWLM</i> application. (<i>FortiWLM > Reports & Notify > User Preference > Notification Profiles</i>). • Notification Message: Type a notification message (max 64 chars). • Stream: Select the stream from the drop-down list. The options are as follows: <ul style="list-style-type: none"> • Up: Upstream traffic refers to data that is sent from a computer or network. (default) • Down: Downstream traffic refers data that is received by a computer or network. <p>The “<i>Advanced Options</i>” on page 330 are displayed when the Baseline Type, Measured is selected.</p>
Throughput - UDP	

Field	Descriptions
Baseline Type	<p>Select the Baseline Type from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> Configured: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields: <ul style="list-style-type: none"> Throughput: Enter the <i>Throughput</i> value (1-150 Mbps). Stream: Select the stream from the drop-down list. The options are as follows: <ul style="list-style-type: none"> Up: <i>Upstream</i> traffic refers to data that is sent from a computer or network. (default) Down: <i>Downstream</i> traffic refers data that is received by a computer or network. Measured: The <i>Measured</i> option allows you to run the baseline. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (<i>Connectivity</i>, <i>Throughput</i> or <i>Voice</i>) will take precedence over this test. This option enables the following fields: <ul style="list-style-type: none"> Notification: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list. Notification Profile: Select the notification profile from the drop-down list. The notification profiles are configured in the <i>FortiWLM</i> application. (<i>FortiWLM</i> > <i>Reports & Notify</i> > <i>User Preference</i> > <i>Notification Profiles</i>). Notification Message: Type a notification message (max 64 chars). Stream: Select the stream from the drop-down list. The options are as follows: <ul style="list-style-type: none"> Up: <i>Upstream</i> traffic refers to data that is sent from a computer or network. (default) Down: <i>Downstream</i> traffic refers data that is received by a computer or network. <p>The “<i>Advanced Options</i>” on page 330 are displayed when the Baseline Type, Measured is selected.</p>

Field	Descriptions
Test Type - Voice	
Baseline Type	<p>Select the <i>Baseline Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> Configured: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields: <ul style="list-style-type: none"> Latency (Connectivity test only): Latency is an expression of how much time is taken for a packet of data to get from one designated point to another. A low latency network connection generally experiences small delay times, while a high latency connection generally suffers from long delays. Provide a latency value for a baseline connectivity test (1-1000ms). The default value is 100. Packet Loss % (Connectivity test only): Packet loss is the failure of one or more transmitted packets to arrive at their destination. Enter the packet loss % value. The default is 0. Number of Calls: Enter a value for the number of calls (1-15). Measured: The Measured option allows you to run the baseline. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (<i>Connectivity, Throughput or Voice</i>) will take precedence over this test. This option enables the following fields:

Field	Descriptions
	<ul style="list-style-type: none"> • Notification: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list. • Notification Profile: Select the notification profile from the drop-down list. The notification profiles are configured in the <i>FortiWLM</i> application. (<i>FortiWLM > Reports & Notify > User Preference > Notification Profiles</i>). • Notification Message: Type a notification message (max 64 chars). • Number of Calls: Enter a value for the <i>Number of Calls</i> (1-15). <p>The “<i>Advanced Options</i>” on page 330 are displayed when the Baseline Type, Measured is selected.</p>
Advanced Options	
Retries	Type the number of <i>Retries</i> . This field allows you to configure the number of retries when SAM tests fail for an <i>ESS Profile</i> . The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the <i>Timeout</i> value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the <i>Redo Failed Tests</i> option, the tests get repeated for failed tests.
Tunnel Type	<p>Select the <i>Tunnel Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Ether IP: This is the default tunnel. Here the data packets are sent through the ether IP tunnel, between the <i>FortiWLM</i> and AP. • Ether UDP: Here the data packets are sent through the Ether UDP tunnel, between the <i>FortiWLM</i> and AP.
Signal Strength Check	<p>Select the <i>Signal Strength Check</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • On: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the signal strength threshold is examined. The signal strength threshold must be within (-85 to -30 dBm). The default value is -70dBm. • Off: The surroundings are not examined for the presence or absence of the neighbor APs.

Field	Descriptions
Signal Strength Threshold	The <i>Signal Strength Threshold</i> is applicable only when the <i>Signal Strength Check</i> option is <i>On</i> . The <i>Signal Strength Threshold</i> must be within (-85 to -30 dBm). The default value is -70dBm.
Ping test before Throughput	Select the <i>Ping test before Throughput</i> from the drop-down list. The options are as follows: <ul style="list-style-type: none"> • On: The ping is run before running the throughput test. • Off: The ping is not run before the throughput test. <p>This option is <i>On</i> by default. The throughput tests can still be run when the ICMP is blocked by turning the ping Off.</p>
Buffer Length	Enter the <i>Buffer Length</i> value (1KB-1MB). <i>Buffer Length</i> is the amount of data to be sent. The default value is 128 KB.
Window Size	Enter a value for the <i>Window Size</i> . (8KB-128KB). The <i>Window Size</i> is the TCP window size. The default value is 85.3 KB.
Packet Size	Enter the <i>Packet Size value</i> (1 -1280 Bytes). The <i>Packet Size</i> is the size of UDP data packet to be sent. The default Value 1024 Bytes. Range is (1-1280 Bytes).
Buffer Size	Enter a value for the <i>Buffer Size</i> . (8KB-128KB). The buffer size is the socket send buffer size (SO_SNDBUF). The default value is 85.3KB.
Bandwidth	Enter the <i>Bandwidth</i> value (1Kbps-50 Mbps). The bandwidth is the amount of UDP data to be pumped in bits/sec. The default value is 5Mbps.
Logging Detail	Select the <i>Logging Detail</i> from the drop-down list. The options are as follows: <ul style="list-style-type: none"> • Log only critical messages: This option logs only the critical messages. • Log all messages: This option logs all the messages.

3. Select at least one cell for the baseline test and select the *Include* option.



If you receive the error “Please include at least one cell for baseline test” that means that no cell has been selected. Go back and select them.

If there are no rows or columns listed, then the selected controller has no APs with IP address.

4. Click *Save* to save the baseline as configured baseline (indicated in the *Baseline Type* column) at the top of the list.
5. Click *Save & Run* to save and run the baseline as measured baseline. The *Save & Run* option is displayed only for the *Measured Baseline Type*.

If you have selected the *Measured Baseline Type*, a virtual client with its own IP address runs on each interface, each profile, measuring the current values for the selected controller. The completed test results of the measured baseline test results are displayed on the baseline tests screen. You can schedule a throughput test, once a baseline test is established.



If you stop any test, you must restart the test from the beginning.

Scheduling Tests

The tests are the central activity of the *SAM* application that is dealt the most. A baseline test is performed occasionally, but the scheduled tests and their results are monitored constantly. The test results can be notified through email.

Scheduled tests are measured against a baseline test for *Connectivity*, *Throughput*, and *Voice* using the configurations provided while creating the test to link the three. Only *APs* and *SSIDs* within the baseline test is measured in subsequent tests. The tests that are run without a corresponding baseline displays the status as *No Baseline*.

Tests are measured against the below mentioned values for *Voice*.

- **Good:** Packet Loss = 0%, RTT <= 100ms
- **Fair:** Packet Loss < 2%, RTT <= 120ms
- **Bad:** Packet Loss > 2% or RTT > 120ms

Add a Scheduled Test

You can configure many number of scheduled tests against a baseline test. You can either create a test, disable or enable it to activate immediately. Tests are scheduled on a regular interval and the test results are verified by viewing the results or by scheduling an email notification.

To add a *Scheduled Test*, follow these steps:

1. Navigate to *Configure > Tests > Scheduled Tests > Add Test*.
Figure 125 on page 334 illustrates the *Add Scheduled Test* screen.
2. In the *Scheduled Test - Add* screen, provide the following details for the *Scheduled Test - Add*.

Figure 125: Schedule Test - Add

Schedule Tests

Scheduled Test - Add

Name*

Doc

(1 - 31 chars max)

Test Type

Connectivity

Controller Name


172.18.60.14

Controller IP

172.18.60.14

Baseline Test Name

testrad




Interval

Once

Status

Enabled

Start Time*



Notification

None

Notification Profile

SAM4dot0

Notification Message

(max 64 chars)

- Advanced Options

Latency Good Threshold*

50

(1 - 10000 ms)

Latency Fair Threshold*

100

(1 - 10000 ms)

Packet Loss Good Threshold*

0

(0 - 100 %)

Packet Loss Fair Threshold*

30

(0 - 100 %)

Retries*

2

(0-2)

Timeout*

30

(10-30)

Redo Failed Tests

☒

Tunnel Type

Ether IP

Signal Strength Check

On

Signal Strength Threshold

-70 dBm

Logging Detail

Log only critical messages

Save

Cancel

Field	Description
Name	Provide a name of the scheduled test primarily for usage. The name consists of up to 31 characters, including numbers, letters, capital letters, and special characters.

Field	Description
Test Type	<p>Select the <i>Test Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> Connectivity: <i>Connectivity</i> describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another. The selection of the <i>Test Type</i> as <i>Connectivity</i> determines the rest of the options on the page. Refer to “Test Type - Connectivity” on page 338. Throughput: <i>Throughput</i> is the amount of data moved successfully from one place to another in a given time period. The selection of the <i>Test Type</i> as <i>Throughput</i> determines the rest of the options on the page. The throughput test type can further be divided as follows: <ul style="list-style-type: none"> Throughput TCP (Transmission Control Protocol). Refer to “Throughput - TCP” on page 340 Throughput UDP (User Datagram Protocol). Refer to “Throughput - UDP” on page 342 Voice: <i>Voice</i> is simulated using multiple thread of ping traffic. The selection of the <i>Test Type</i> as <i>Voice</i> determines the rest of the options on the page. Refer to “Test Type - Voice” on page 344. The scheduled tests that run on the selected controller must match the test type in order to measure against the baseline.
Controller Name	<p>Select the <i>Controller Name</i> or the <i>Host name</i> from the drop-down list. The controller name displayed is the controller mapped to the <i>FortiWLM</i> inventory; the test runs on the indicated controller.</p>
Controller IP	<p>Select the <i>Controller IP</i> address from the drop-down list. The controller IP address displayed is the controller mapped to the <i>FortiWLM</i> inventory; the test runs on the indicated controller.</p>
Baseline Test Name	<p>Select a <i>Baseline Test Name</i> from the drop-down list. This value links a baseline to this test. The test will be run only for the <i>IF ID/ESS Profile</i> listed in the baseline. You can modify the <i>IF ID/ESS Profile</i> named in the baseline by selecting <i>Edit icon</i> next to the drop-down list.</p> <p>Note: Only the baseline tests with <i>Completed</i> status is displayed.</p>

Field	Description
Interval	<p>Select an <i>Interval</i> type from the drop-down list. The following are the options:</p> <ul style="list-style-type: none"> • Instant: This option enables to run the scheduled test once, immediately after it is saved. The tests with the <i>Instant</i> interval type gets displayed on the <i>Ongoing Tests</i> screen (<i>SAM > Monitor > Tests > Ongoing</i>). It does not get displayed on the <i>Schedule Tests</i> screen. • Once: This option enables to run the scheduled test immediately after it is saved. The following fields are displayed upon selection. <ul style="list-style-type: none"> • Status: Select <i>Enabled</i> or <i>Disabled</i> from the drop-down list. The <i>Enabled</i> option (default) activates a test. The <i>Disabled</i> option does not run the test. • Start Time: Select the <i>Start Time</i> from the <i>Calendar</i> in <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format. • Continuous: This option enables to execute the scheduled test continuously till you disable the test. The following fields are displayed upon selection. <ul style="list-style-type: none"> • Status: Select <i>Enabled</i> or <i>Disabled</i> from the drop-down list. The <i>Enabled</i> option (default) activates a test. The <i>Disabled</i> option does not run the test. • Hourly: This option enables to execute the scheduled test every hour at the time given <i>Start Time</i>. The following fields are displayed upon selection. <ul style="list-style-type: none"> • Status: Select <i>Enabled</i> or <i>Disabled</i> from the drop-down list. The <i>Enabled</i> option (default) activates a test. The <i>Disabled</i> option does not run the test. • Start Time: Select the <i>Start Time</i> from the <i>Calendar</i> in <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format. • Daily: This option enables to execute the scheduled test every day at the given <i>Start Time</i>. The following fields are displayed upon selection. <ul style="list-style-type: none"> • Status: Select <i>Enabled</i> or <i>Disabled</i> from the drop-down list. The <i>Enabled</i> option (default) activates a test. The <i>Disabled</i> option does not run the test. • Start Time: Select the <i>Start Time</i> from the <i>Calendar</i> in <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format.

Field	Description
	<ul style="list-style-type: none"> • Weekly: This option enables to execute the scheduled test every week as per the scheduled day and time of the week indicated in the <i>Start Time</i> field. The following fields are displayed upon selection. • Status: Select <i>Enabled</i> or <i>Disabled</i> from the drop-down list. The <i>Enabled</i> option (default) activates a test. The <i>Disabled</i> option does not run the test. • Start Time: Select the <i>Start Time</i> from the <i>Calendar</i> in <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format.
Notification	<p>Select the <i>Notification</i> from the drop-down list. This (SAM defined tests only) determines if anyone is to be emailed when one or more threshold violations are noticed in a test. The following are the types:</p> <ul style="list-style-type: none"> • None: Never notify anyone. • Critical: Email only when the <i>Bad Threshold</i> value in a <i>Scheduled Test</i> is met or exceeded at least once. • Major: Email only when the <i>Good Threshold</i> value in a <i>Scheduled Test</i> falls below the setting at least once. • Information: Email irrespective of the results threshold.
Notification Profile	<p>Select the <i>Notification Profile</i> from the drop-down list. The notification profiles are configured in the <i>FortiWLM</i> application. (<i>FortiWLM > Reports & Notify > User Preference > Notification Profiles</i>). Indicate a profile name here; all email addresses in the profile will be sent the <i>Notification Message Subject</i> as indicated.</p>
Notification Message	<p>Type a notification message (max 64 chars).</p>
Advanced Options	<p>Optional. Click the <i>Advanced Options</i>. The following information is displayed for the respective Test Type.</p>

Field	Description
Test Type - Connectivity	
By selecting the <i>Test Type</i> as <i>Connectivity</i> , the following fields appear in the <i>Advanced Options</i> :	
Latency Good Threshold	Type a value for the <i>Latency Good Threshold</i> . The latency value is between 1 ms and 10000 ms. Latency recorded at or below this setting is considered to be good.
Latency Fair Threshold	Type a value for the <i>Latency Fair Threshold</i> . The latency value is between 1 ms and 10000 ms. Latency recorded at or below this setting is considered fair until latency crosses the threshold for good (set above). The latency above this number is marked as bad.
Packet Loss Good Threshold	Type a value for <i>Packet Loss Good Threshold</i> . This is a percentage below which a packet loss result is considered good. This number is the default threshold for all tests. If the baseline for a particular test displays a poorer number, that becomes the actual threshold for that test.
Packet Loss Bad Threshold	Type a value for <i>Packet Loss Bad Threshold</i> . This is a percentage above which a packet loss result is considered bad. This number is the default threshold for all tests. If the baseline for a particular test displays a poorer number, that becomes the actual threshold for that test. A number between the good and bad threshold is considered fair.
Retries	Type the number of <i>Retries</i> . This field allows you to configure the number of retries when SAM tests fail for an <i>ESS Profile</i> . The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the <i>Timeout</i> value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the <i>Redo Failed Tests</i> option the tests get repeated for failed tests. If the value for <i>Timeout</i> (above) is exceeded, retry the test again until the value of <i>Retries</i> (above) is met.
Tunnel Type	Select the <i>Tunnel Type</i> from the drop-down list. The options are as follows: <ul style="list-style-type: none"> • Ether IP: This option is the default tunnel. Here the data packets are sent through the Ether IP tunnel, between the <i>FortiWLM</i> and AP. • Ether UDP: Here the data packets are sent through the Ether UDP tunnel, between the <i>FortiWLM</i> and AP.

Field	Description
Signal Strength Check	<p>Displays the <i>Signal Strength Check</i>. The options are as follows:</p> <ul style="list-style-type: none"> • On: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the <i>Signal Strength Threshold</i> is examined. The <i>Signal Strength Threshold</i> must be within (-85 to -30 dBm). The default value is -70dBm. • Off: The surroundings are not examined for the presence or absence of the neighbor APs.
Signal Strength Threshold	<p>Displays the <i>Signal Strength Threshold</i>. This is displayed only when the <i>Signal Strength Check</i> option is <i>On</i>. The <i>Signal Strength Threshold</i> must be within (-85 to -30 dBm). The default value is -70dBm.</p>
Logging Detail	<p>Select the <i>Logging Detail</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Log only critical messages: This option logs only the critical messages. • Log all messages: This option logs all the messages.

Field	Description
Throughput - TCP	
By selecting the <i>Test Type</i> as <i>Throughput-TCP</i> , the following fields appear in the <i>Advanced Options</i> :	
Throughput Good Threshold	<p>Type a value for the <i>Throughput Good Threshold</i>. When the range (0 - 100%) is met or exceeded during a test, throughput is good and no counters are incremented. When throughput value falls below the range, but not below the value of the <i>Throughput Fair Threshold</i> (see below) the throughput is considered to be fair and the counter for fair throughput is incremented for this test.</p> <p>For Example: Set the good throughput threshold at 20% and fair throughput threshold at 10%. In that case, any throughput from 10% to 20% is considered fair and anything above 20% is considered good. A bad throughput is anything below 10%.</p>
Throughput Fair Threshold	Type a value for the <i>Throughput Fair Threshold</i> . When throughput is below the range, throughput is considered as bad and the counter for bad throughput is incremented for the test.
Retries	Type the number of <i>Retries</i> . This field allows you to configure the number of retries when SAM tests fail for an <i>ESS Profile</i> . The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the <i>Timeout</i> value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the <i>Redo Failed Tests</i> option. If the value for <i>Timeout</i> (above) is exceeded, retry the test again until the value of <i>Retries</i> (above) is met.
Tunnel Type	<p>Select the <i>Tunnel Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Ether IP: This is the default tunnel. Here the data packets are sent through the Ether IP tunnel, between the <i>FortiWLM</i> and AP. • Ether UDP: Here the data packets are sent through the Ether UDP tunnel, between the <i>FortiWLM</i> and AP.
Signal Strength Check	<p>Displays the <i>Signal Strength Check</i>. The options are as follows:</p> <ul style="list-style-type: none"> • On: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the Signal Strength Threshold is examined. The Signal Strength Threshold must be within (-85 to -30 dBm). The default value is -70dBm. • Off: The surroundings are not examined for the presence or absence of the neighbor APs.

Field	Description
Signal Strength Threshold	Displays the <i>Signal Strength Threshold</i> . This is displayed only when the <i>Signal Strength Check</i> option is <i>On</i> . The <i>Signal Strength Threshold</i> must be within (-85 to -30 dBm). The default value is -70dBm.
Ping test before Throughput	<p>Select the <i>Ping test before Throughput</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • On: The ping is run before running the throughput test. The throughput tests are conducted based on the success of the ping. • Off: The ping is not run before the throughput test. This option is <i>On</i> by default. The throughput tests can still be run when the ICMP is blocked by turning the ping Off.
Logging Detail	<p>Select the Logging Detail from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Log only critical messages: This option logs only the critical messages. • Log all messages: This option logs all the messages.

Field	Description
Throughput - UDP	
By selecting the <i>Test Type</i> as <i>Throughput - UDP</i> , the following fields appear in the <i>Advanced Options</i> :	
Throughput Good Threshold	<p>Type a value for the <i>Throughput Good Threshold</i>. When the range (0 - 100%) is met or exceeded during a test, throughput is good and no counters are incremented. When throughput value falls below the range, but not below the value of the <i>Throughput Fair Threshold</i> (see below), the throughput is considered to be fair and the counter for fair throughput is incremented for this test.</p> <p>For Example: Set the good throughput threshold at 20% and fair throughput threshold at 10%. In that case, any throughput from 10% to 20% is considered fair and anything 20% or more is good. Bad throughput is anything below 10%.</p>
Throughput Fair Threshold	Type a value for the <i>Throughput Fair Threshold</i> . When throughput is below the range, throughput is considered as bad and the counter for bad throughput is incremented for the test.
Retries	Type the number of <i>Retries</i> . This field allows you to configure the number of retries when SAM tests fail for an <i>ESS Profile</i> . The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the <i>Timeout</i> value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the <i>Redo Failed Tests</i> option. If the value for <i>Timeout</i> (above) is exceeded, retry the test again until the value of <i>Retries</i> (above) is met.
Tunnel Type	<p>Select the <i>Tunnel Type</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Ether IP: This is the default tunnel. Here the data packets are sent through the Ether IP tunnel, between the <i>FortiWLM</i> box and AP. • Ether UDP: Here the data packets are sent through the Ether UDP tunnel, between the <i>FortiWLM</i> box and AP.
Signal Strength Check	<p>Displays the <i>Signal Strength Check</i>. The options are as follows:</p> <ul style="list-style-type: none"> • On: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the Signal Strength Threshold is examined. The Signal Strength Threshold must be within (-85 to -30 dBm). The default value is -70dBm. • Off: The surroundings are not examined for the presence or absence of the neighbor APs.

Field	Description
Signal Strength Threshold	Displays the Signal Strength Threshold. This is displayed only when the Signal Strength Check option is On . The Signal Strength Threshold must be within (-85 to -30 dBm). The default value is -70dBm.
Ping test before Throughput	<p>Select the <i>Ping test before Throughput</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • On: The ping is run before running the throughput test. The throughput tests are conducted based on the success of the ping. • Off: The ping is not run before the throughput test. This option is <i>On</i> by default. The throughput tests can still be run when the ICMP is blocked by turning the ping Off.
Logging Detail	<p>Select the <i>Logging Detail</i> from the drop-down list. The options are as follows:</p> <ul style="list-style-type: none"> • Log only critical messages: This option logs only the critical messages. • Log all messages: This option logs all the messages.

Field	Description
Test Type - Voice	
By selecting the <i>Test Type</i> as <i>Voice</i> , the following fields appear in the <i>Advanced Options</i> :	
Number of Calls	Type a value for the <i>Number of Calls</i> (1-100). Note: The <i>Number of Calls</i> option is disabled or non editable, as its values are taken from the selected baseline (only for viewing).
Retries	Type the number of <i>Retries</i> . If the test fails, try again this number of times (0 - 2).
Timeout	Type the <i>Timeout</i> value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the <i>Redo Failed Tests</i> option. If the value for <i>Timeout</i> (above) is exceeded, retry the test again until the value of <i>Retries</i> (above) is met.
Tunnel Type	Select the <i>Tunnel Type</i> from the drop-down list. The options are as follows: <ul style="list-style-type: none"> • Ether IP: This is the default tunnel. Here the data packets are sent through the <i>Ether IP</i> tunnel, between the <i>FortiWLM</i> and AP. • Ether UDP: Here the data packets are sent through the Ether UDP tunnel, between the <i>FortiWLM</i> and AP.
Signal Strength Check	Displays the <i>Signal Strength Check</i> . The options are as follows: <ul style="list-style-type: none"> • On: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the <i>Signal Strength Threshold</i> is examined. The <i>Signal Strength Threshold</i> must be within (-85 to -30 dBm). The default value is -70dBm. • Off: The surroundings are not examined for the presence or absence of the neighbor APs.
Signal Strength Threshold	Displays the <i>Signal Strength Threshold</i> . This is displayed only when the <i>Signal Strength Check</i> option is <i>On</i> . The <i>Signal Strength Threshold</i> must be within (-85 to -30 dBm). The default value is -70dBm.
Logging Detail	Select the <i>Logging Detail</i> from the drop-down list. The options are as follows: <ul style="list-style-type: none"> • Log only critical messages: This option logs only the critical messages. • Log all messages: This option logs all the messages.

3. Click **Save**. The test added is displayed on the *Completed Tests* of the *Monitor Dashboard*.

The test will run as indicated; multiple tests can run simultaneously for different controller IPs. SA2000 can run up to 14 overlapping tests and SA200 can run up to seven. If you look at the directions for a test, you'll see that the Interval can be set to Instant.

Modify a Test Criteria

To edit the criterion for a *Scheduled Test*, follow the below steps:

1. Navigate to *Configure > Tests > Scheduled Tests > select a test > Edit*.
2. In the *Scheduled Test - Edit* screen, perform the changes as required.
3. Select *Save*. The updated test is displayed on the *Scheduled Test* screen.

Enable a Test

To enable a scheduled test, follow these steps:

1. Navigate to *Configure > Tests > Scheduled Tests*.
2. Select one or more tests by clicking the radio button to activate the test.

Infrastructure

The security permissions (*User Name* and *Password*) for the RADIUS based WPA, WPA2, 802.1x, Mixed *ESS Profiles* and *Captive Portal* must be configured in *SAM*. The below procedure provides a brief description to configure security permissions for *SAM client* and *Captive Portal*.

SAM Clients

The security permissions (*User Name* and *Password*) for the RADIUS based WPA, WPA2, 802.1x, Mixed *ESS Profiles* must be configured.

Add Security Permission for SAM Clients















To add security permission for a *SAM* client, follow these steps:

1. Navigate to *Configure > Infrastructure > SAM Clients > Add option*.

See [Figure 126 on page 346](#) illustrates the *SAM Clients* screen.

Figure 126: SAM Clients

SAM Clients

SAM Clients + Add				
	Controller Name	Controller IP	SSID	User Name
 	172.18.60.14	172.18.60.14	Drav-bug39590	radius
 	172.18.71.199	172.18.71.199	sam1_dot1x	sam
 	172.18.71.199	172.18.71.199	sam1_dot1x128	sam
 	172.18.71.199	172.18.71.199	sam1_wpa2	sam
 	172.18.79.199	172.18.79.199	tj-dot1x	sam
 	172.18.79.199	172.18.79.199	tj-wpa	sam
 	172.18.79.199	172.18.79.199	tj-wpa2	sam

2. In the *Add SAM Client* pop-up, provide the following details:

Field	Description
Controller Name	Select the controller name that is associated to the <i>RADIUS Key</i> record.
Controller IP	Select the controller IP address that is associated to the <i>RADIUS Key</i> record.
SSID	Type the SSID that is associated to the WPA, WPA2, 802.1x, Mixed <i>ESS Profiles</i> .

Field	Description
User Name	Type a user name used by the SAM client on the selected SSID, for example Fortinet guest. The special character @ symbol is allowed for configuring the user name.
Password	Type the <i>Password</i> associated with the user identity.

3. Click **Save**. The client security is now configured.

Edit Security Permission for SAM Clients

To edit the security permission for a *SAM* client, follow the below steps:

1. Navigate to *Configure > Infrastructure > SAM Clients*.
2. Select a client security followed by selecting the *Edit* option.
3. In the *Edit SAM Client* pop-up, provide the following details:

Field	Description
Controller Name	Displays the controller name that is associated to the <i>RADIUS</i> Key record.
Controller IP	Displays the controller IP address that is associated to the <i>RADIUS</i> Key record.
SSID	Modify the SSID that is associated to the WPA, WPA2, 802.1x, Mixed <i>ESS Profiles</i> .
User Name	Modify the user name used by the SAM client on the selected SSID.
Password	Modify the <i>Password</i> associated with the user identity.

4. Click **Save**. The updated client security is now displayed on the *SAM Clients* screen.

Delete Security Permission for SAM Clients

To delete security permission for a *SAM* client, follow these steps:

1. Navigate to *Configure > Infrastructure > SAM Clients*.
2. Select a client security followed by selecting the *delete* icon. A conformation message is displayed to continue the deletion.
3. Select *OK* to proceed and *Cancel* to cancel the deletion.

Add Security Permissions for Captive Portal

If you want to provide limited wireless access to a group of users, use *Captive Portal*. *Captive Portal* is a feature designed to isolate temporary users on a network. For example, guests in a company or students using a library. If *Captive Portal* is enabled, the *HTTP* protocol over *Secure Socket Layer* (SSL, also known as *HTTPS*) provides an encrypted login interchange with the *RADIUS* server until the user is authenticated and authorized. During this interchange, all traffic with the client station except *DHCP*, *ARP*, and *DNS* packets is dropped until access is granted. If access is not granted, the user is unable to leave the *Captive Portal* login page. If access is granted, the user is released from the *Captive Portal* page and is allowed to enter the *WLAN*.

The security for *SAM* virtual client must be configured, as it connects to the *Wireless LAN* and runs the connectivity and performance tests subsequently. This implies that the *SSID* identified consists of an enterprise-mode security profile involving *RADIUS*. The security for *SAM* virtual client is performed by configuring the *Captive Portal Users and Types* in the *SAM* web UI.

Captive Portal Types

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Types > Add option*.

See [Figure 127 on page 348](#) illustrates the *Add/Edit Captive Portal Type* screen.

Figure 127: *Add/Edit Captive Portal Type*

Add/Edit Captive Portal Type

Identifier

samcaptive

Test URL *

www.google.com

(1 - 255 chars max)

Match String *

vpn

(1 - 64 chars max)

Success String *

Succeeded

(1 - 64 chars max)

Failure String *

Authentication Failed

(1 - 64 chars max)

Save

Cancel

2. In the *Add/Edit Captive Portal Type* pop-up, provide the following information:

Field	Description
Identifier	Provide the name for a given <i>Captive Portal</i> . Later, when you configure the <i>Captive Portal</i> users, use this same identifier. This links the <i>Identification String</i> , <i>Success String</i> & <i>Failure String</i> to the users.

Field	Description
Test URL	Provide the web site that the client tries to access, For example: google.com
Match String	Provide a identification string from the <i>Captive Portal's</i> login form. For the <i>Fortinet Captive Portal</i> , the default value is (lowercase only) vpn.
Success String	Provide the string from the <i>Captive Portal's login</i> form success ID confirmation that appears on the page immediately following a successful login. For the <i>Fortinet Captive Portal</i> , the default value is Succeeded.
Failure String	Provide the confirmation that appears on the page immediately following an incorrect login. For the default <i>Fortinet Captive Portal</i> , the value is <i>Authentication Failed</i> .

3. Select *Save*. The new *Captive Portal* is included and is displayed on the *Captive Portals* screen.

Edit Captive Portal Types

To edit the security permission for a *SAM* client, follow the below steps:

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Types*.
2. Select a captive portal type followed by selecting the *Edit* option.
3. In the *Add/Edit Captive Portal Type* pop-up, provide the following details:

Field	Description
Identifier	Displays the name for a given <i>Captive Portal</i> .
Test URL	Modify the web site that the client tries to access, For example: google.com
Match String	Modify the identification string from the <i>Captive Portal's</i> login form. For the <i>Fortinet Captive Portal</i> , the default value is (lowercase only) vpn.
Success String	Modify the string from the <i>Captive Portal's login</i> form success ID confirmation that appears on the page immediately following a successful login. For the <i>Fortinet Captive Portal</i> , the default value is Succeeded.
Failure String	Modify the confirmation that appears on the page immediately following an incorrect login. For the default <i>Fortinet Captive Portal</i> , the value is <i>Authentication Failed</i> .

4. Click *Save*. The updated captive portal type is now displayed on the *Captive Portals* screen.

Delete Captive Portal Types

To delete the captive portal types, follow these steps:

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Types*.
2. Select a captive portal type followed by selecting the *delete* icon. A *confirmation* message is displayed to continue the deletion.
3. Select *OK* to proceed and *Cancel* to cancel the deletion.



The identifier that is still in association with user or users cannot be deleted. The corresponding users must be deleted first.

Captive Portal Users

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Users > Add option*.

See [Figure 128 on page 350](#) illustrates the *Captive Portal Add User* screen.

Figure 128: Add Captive Portal User

The screenshot shows a dialog box titled "Add Captive Portal User". It contains the following fields:

- Controller Name:** A drop-down menu showing "172.19.37.220".
- Controller IP:** A drop-down menu showing "172.19.37.220".
- Identifier*:** A text field containing "samcaptive" with a note "(1 - 31 chars max)".
- SSID*:** A text field containing "Ha207clear" with a note "(1 - 31 chars max)".
- User Name*:** A text field containing "Test" with a note "(1 - 31 chars max)".
- Password*:** A text field with masked characters "...." and a note "(1 - 64 chars max)".

At the bottom of the dialog are two buttons: "Save" and "Cancel".

2. In the *Add Captive Portal User* pop-up, provide the following information:

Field	Description
Controller Name	Select the Controller Name from the drop-down list.
Controller IP	Select the Controller IP from the drop-down list.
Identifier	Provide a Captive portal type to which this SSID is linked; use the same identifier that you used to configure the Captive Portal type (see above).

Field	Description
SSID	Provide a identification string from the <i>Captive Portal's</i> login form. For the <i>Fortinet Captive Portal</i> , the default value is (lowercase only) vpn.
User Name	Provide the string from the <i>Captive Portal's login</i> form success ID confirmation that appears on the page immediately following a successful login. For the <i>Fortinet Captive Portal</i> , the default value is Succeeded.
Password	Provide the confirmation that appears on the page immediately following an incorrect login. For the default <i>Fortinet Captive Portal</i> , the value is <i>Authentication Failed</i> .

3. Select **Save**. The new *Captive Portal User* is included.

Edit Captive Portal Users

To edit the security permission for a *SAM* client, follow the below steps:

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Users*.
2. Select a captive portal users followed by selecting the *Edit* option.
3. In the *Edit Captive Portal User* pop-up, provide the following details:

Field	Description
Controller Name	Displays the <i>Controller Name</i> .
Controller IP	Displays the <i>Controller IP</i> address
Identifier	Modify the name for a given <i>Captive Portal</i> .
SSID	Modify the identification string from the <i>Captive Portal's</i> login form. For the <i>Fortinet Captive Portal</i> , the default value is (lowercase only) vpn.
User Name	Modify the string from the <i>Captive Portal's login</i> form success ID confirmation that appears on the page immediately following a successful login. For the <i>Fortinet Captive Portal</i> , the default value is Succeeded.
Password	Modify the confirmation that appears on the page immediately following an incorrect login. For the default <i>Fortinet Captive Portal</i> , the value is <i>Authentication Failed</i> .

4. Click **Save**. The updated captive portal user is now displayed on the *Captive Portals* screen.

Delete Captive Portal Users

To delete the captive portal types, follow these steps:

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Users*.
2. Select a captive portal user followed by selecting the *delete* icon. A *confirmation* message is displayed to continue the deletion.
3. Select *OK* to proceed and *Cancel* to cancel the deletion.

Get MACs

MAC filtering controls a user station's access to the WLAN by permitting or denying access based on specific MAC addresses. A MAC address is unique to each IEEE 802-compliant networking device. In 802.11 wireless networks, network access can be controlled by permitting or denying a specific station MAC address, assigned to its wireless NIC card, from attempting to access the WLAN.

The *Get MACs* feature allows you to procure the virtual clients MAC addresses for the selected controller.

To find a controller's AP MAC addresses, follow these steps:

1. Navigate to *Configure > Infrastructure > Get MACs*.
2. In the MAC Addresses of AP Interfaces screen, select a *Controller Name/ Controller IP* address from the drop-down list and click one of the following buttons.

See [Figure 129 on page 353](#) illustrates the *MAC Addresses of AP Interfaces* screen.

- **Show MACs:** A list of virtual *Client MAC* addresses for the selected controller is displayed.
When you click the *Show MACs* for the first time, the server gathers all the client MAC addresses from each AP connected to the controller and stores the data. The time taken to display the MACs, depends on the number of APs connected to the controller. The next time you select that controller and click *Show MACs*, the list from the stored file appears quickly.
- **Update MACs:** This option refreshes the AP MAC list and provide the updated MAC list. Click *Update MACs* to procure the updated MAC list.
- **Save MACs:** The updated AP MAC addresses can be downloaded by selecting the *Save MACs* option. The MAC addresses list can also be uploaded to the selected controller to grant access or deny access for MAC filtering.

Figure 129: MAC Addresses of AP Interfaces

MAC Addresses Of AP Interfaces

Controller Name172.19.37.220

Controller IP172.19.37.220

Show MACs

Update MACs

AP Interfaces MACs				Save MACs
AP ID	AP Name	Interface Name	MAC	
6	AP-6	AP-6-1	06:00:31:0e:00:59	
6	AP-6	AP-6-2	06:00:32:0e:00:59	
4	AP-4	AP-4-1	06:00:31:0e:23:8d	
1	AP-1	AP-1-1	06:00:31:09:98:11	
1	AP-1	AP-1-2	06:00:32:09:98:11	
3	AP-3	AP-3-1	06:00:31:0e:23:4c	
2	AP-2	AP-2-1	06:00:31:09:ac:1b	
2	AP-2	AP-2-2	06:00:32:09:ac:1b	
5	AP-5	AP-5-1	06:00:31:0e:00:4b	
5	AP-5	AP-5-2	06:00:32:0e:00:4b	

11 Monitoring SAM

Dashboard

The *SAM Dashboard* provides a rich and interactive view of pertinent wireless data on a single screen. The various charts and statistics described in this chapter helps you determine the overall health of the network.

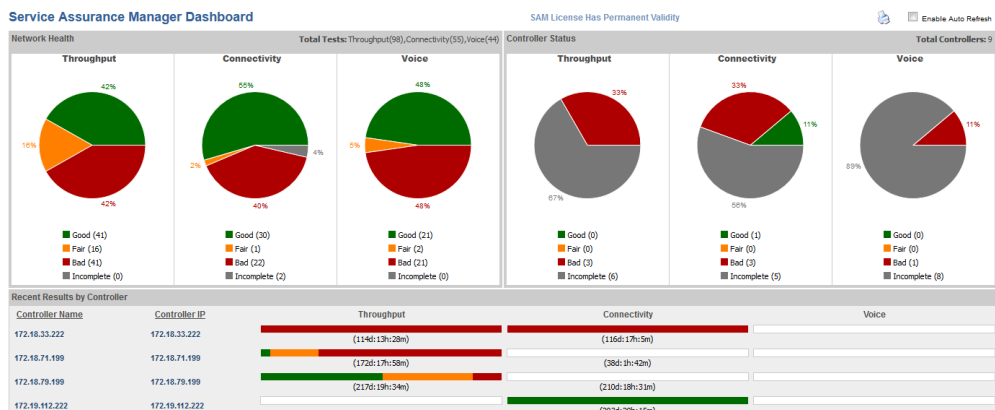
You are provided with two different dashboards; the *Global Dashboard* providing a general information about the network itself and the *Controller Dashboard* displaying the data on a per-controller basis.

Global Dashboard

The *Global Dashboard* provides information pertinent to the overall health of the wireless deployment. From here, you can observe whether there are any general problems in the network (such as low throughput) as well as more specific matters (such as poor voice quality on wireless calls).

[Figure 130 on page 355](#) illustrates the *Global Dashboard View* screen.

Figure 130: Global Dashboard View



The pie charts shown are color-coded to ensure that you can easily determine whether or not a network issue requires attention.

The lower section of the screen displays the same information divided by controller, allowing you to identify any controllers that are generating bad results. Selecting any of the linked controllers shown in the recent results by controller section will direct you to that controller's test information.

Controller Dashboard

The *Controller Dashboard* displays individual statistics for each wireless controller during deployment.

[Figure 131 on page 356](#) illustrates the *Controller Dashboard View* screen.

Figure 131: Controller Dashboard View

Controller Dashboard ☐ Enable Auto

Controller Name	Controller IP	Type	Name	Start Time	Result	Good	Fair	Bad
172.18.33.222	172.18.33.222	Connectivity	222-conn-tam	08/01/2013 19:12	Bad	0	0	4
		Throughput	222-down-tam	08/03/2013 22:49	Bad	0	0	4
		Voice						
172.18.71.199	172.18.71.199	Connectivity	0-parthi-1	10/19/2013 0:31	Controller Offline	0	0	0
		Throughput	psm4	06/06/2013 18:19	Stopped	1	5	12
		Voice						
172.18.78.199	172.18.78.199	Connectivity	Tej-ap19	04/28/2013 17:46	No Neighbors	0	0	0
		Throughput	199-conn-etna	04/22/2013 16:43	Bad	4	3	1
		Voice						
		Connectivity	dfs-gelli	05/06/2013 16:02	Good	1	0	0

The dashboard allows you to view the overall throughput health. Select any of the column table heading to sort the data in the table:

1. Navigate to *Monitor > Dashboard > Controller Dashboard*. The *Controller Dashboard* screen provides a list of all controllers that are tested for *Connectivity*, *Throughput* and *Voice* by *SAM* with the following details:

Field	Description
Controller Name	Displays the controller name. The controller name displayed is the controller mapped to the <i>FortiWLM</i> inventory; the baseline runs on the indicated controller. This is one of the values that links a baseline to subsequent tests.
Controller IP	Displays the controller IP. The controller IP address displayed is the controller mapped to the <i>FortiWLM</i> inventory; the baseline runs on the indicated controller. This is one of the values that links a baseline to subsequent tests.

Field	Description
Type	Displays the test type. The types are as follows: <ul style="list-style-type: none"> • Connectivity • Throughput • Voice
Name	Displays the test name that is provided to each test.
Start Time	Displays the time at which each test started.
Result	Displays the result of the test. The results appear in different color. The result types are as follows: <ul style="list-style-type: none"> • Good • Fair • Bad • Stopped • Offline • No Neighbors • APs Offline • Controller Offline Select a colored result to view the elaborate test details for the selected controller which is displayed in a new window.
Good	Displays the count for <i>Good</i> results. Click on the count that is hyperlinked. The <i>Test Details</i> screen is displayed.
Fair	Displays the count for <i>Fair</i> results. Click on the count that is hyperlinked. The <i>Test Details</i> screen is displayed.
Bad	Displays the count for <i>Bad</i> results. Click on the count that is hyperlinked. The <i>Test Details</i> screen is displayed.
N/A	Displays the results that are not applicable.

Click any *Controller IP* address to view the controller's details that were used to create the charts.

Trends

The *Trends* page provides the graphical representation of the *Completed* and *Failed* recurring tests. The following are the types of Trends Dashboard.

- Results Trends - Refer to [“Results Trends” on page 358](#)
- Failure Trends - Refer to [“Failure Trends” on page 364](#)

Results Trends

Navigate to *Monitor > Trends > Result Trends*. The *Results Trend* page provides the graphical representation of the completed recurring tests.

To view the results trend for the completed tests perform the selections in the following three sections:

- *“Header Section” on page 358*
- *“Trend Graphs Section” on page 360*
- *“Matrix Section” on page 363*

Header Section

The header section consists of the following fields as displayed in the below table:

Field	Description
Controller Name	Provides the complete list of <i>Controller Names</i> for which the test was run. You can either select the <i>Controller Name</i> or the <i>Controller IP</i> . By the selection of either of the options, the other is selected automatically.
Controller IP	Provides the complete list of <i>Controller IPs</i> for which the test was run. You can either select the <i>Controller IP</i> or the <i>Controller Name</i> . By the selection of either of the options, the other is selected automatically.

Field	Description
Test Type	<p>Displays the <i>Test Type</i> as follows:</p> <ul style="list-style-type: none"> • Connectivity: <i>Connectivity</i> describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another. The test result for <i>Connectivity</i> is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt). • Throughput: <i>Throughput</i> is the amount of data moved successfully from one place to another in a given time period. The throughput test type can further be divided as follows: <ul style="list-style-type: none"> • Throughput TCP: The test result for <i>Throughput TCP</i> is displayed in <i>Mbps</i>. • Throughput UDP: The test result for <i>Throughput UDP</i> is displayed in <i>Mbps, % (percentage)</i> for <i>Packet Loss</i> and <i>ms (Millisecond)</i> for <i>Latency</i>. • Voice: <i>Voice</i> is simulated using multiple thread of ping traffic. The selection of the <i>Test Type</i> as <i>Voice</i> determines the rest of the options on the page. The test result for <i>Voice</i> is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt). <p>Note: The connectivity, voice and throughput UDP test type allows you to choose a type of Matrix from the Matrix section. The types are <i>Latency</i> and <i>Packet loss</i>.</p> <p>Select one of the above mentioned <i>Test Type</i> from the drop-down list.</p>
Test Name	<p>Displays the <i>Test Name</i>. Select a test name from the drop-down list.</p>
Start Time	<p>Select the <i>Start Time</i>. The format followed is the <i>mm/dd/yyyy</i> and <i>hh:mm:ss format</i>. The time can be entered manually or by selecting the calendar icon. The calendar is displayed, where the date and time can be modified manually.</p>
End Time	<p>The <i>End Time</i> is automatically selected for the current date. To modify the end time and date, uncheck the <i>Now</i> option and enter the date manually.</p> <p>Else select the calendar icon. The calendar is displayed, where the date and time can be modified manually.</p>

1. Select all the parameters from the above mentioned fields.
2. Select the *Show Trend* button. The trend graph gets plotted in the *Trend Graphs* Section.

3. The charts can be modified according to the selected row or column or single cell or for all the table cells.

Trend Graphs Section

The *Trend Graphs Section* displays the trend of *Good*, *Fair*, *Bad* and *Incomplete* test results of the selected test type and controller within the specified date range.

The following two types of Trend graph results are displayed.

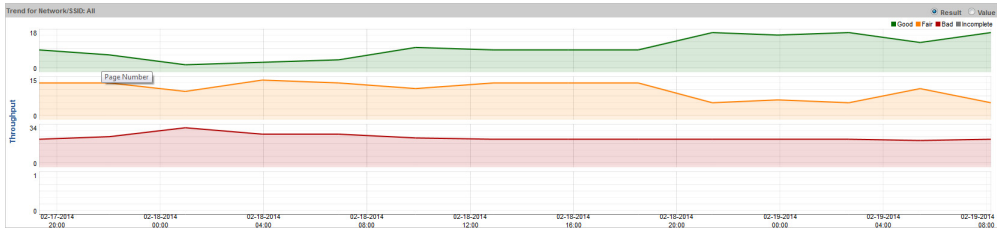
- Results Graph - Refer to “*Result graph*” on page 360
- Value Graph - Refer to “*Value graph*” on page 361

Result graph



The *Result* graph displays the matrix of the test instances. The cell values in the matrix, is the average value for the selected test instance. It displays the incomplete test counts, respectively. The result chart is plotted either by selecting a row or column or single cell or for all table cells. The data for each plotted line in the graph is viewed by hovering the mouse pointer over individual section.



Figure 132 on page 360 illustrates the *Results Trend* graph screen.

Figure 132: Results Graph



The *Date/Time*, *Good*, *Fair*, *Bad*, and *Incomplete* numbers are displayed with four different colors as follows:

Result Type	Description	Color
Good	If the number of tests with fair and bad results is zero, then a test is good.	
Fair	If no test has a bad result and at least one test has a fair result, then a test is fair.	

Result Type	Description	Color
Bad	If there is at least one test with a bad result, then a test is bad.	
Incomplete	If the test stops in between, then the test is incomplete.	

For Example:

The below example provides the completed results of *Throughput TCP* (Test1, Test 2 and Test 3) with their test details. Each test consists of 2 Rows and 2 columns of data, since we have 2 ESS Profiles and 2 AP-Radios:

Test 1			Test 2			Test 3		
IF ID \ ESS Profile	kkp	kkp clear	IF ID \ ESS Profile	kkp	kkp clear	IF ID \ ESS Profile	kkp	kkp clear
AP-1-1	2.7 Mbps	23.7 Mbps	AP-1-1	2.0 Mbps	21.2 Mbps	AP-1-1	2.7 Mbps	16.7 Mbps
AP-1-2	9.7 Mbps	70.1 Mbps	AP-1-2	8.4 Mbps	67.7 Mbps	AP-1-2	10.2 Mbps	66.4 Mbps
AP-2-1	1.8 Mbps	15.8 Mbps	AP-2-1	1.6 Mbps	22.7 Mbps	AP-2-1	2.0 Mbps	19.2 Mbps
AP-2-2	9.2 Mbps	67.7 Mbps	AP-2-2	10.0 Mbps	68.5 Mbps	AP-2-2	10.1 Mbps	68.6 Mbps

From the above mentioned three samples the throughput completed results (Test1, Test 2 and Test 3) with their test details, the number of Good, Fair, Bad and Incomplete are calculated.

Test	Good	Fair	Bad	Incomplete
Test 1	6	2	0	0
Test 2	5	3	0	0
Test 3	5	3	0	0

Value graph

The *Value* graph displays three lines for *Minimum*, *Average* and *Maximum* values for complete test results. The value chart is plotted either by selecting a row or column or single cell or for all table cells. The individual data for each plotted line in the graph can be viewed by hovering the mouse pointer over the section.

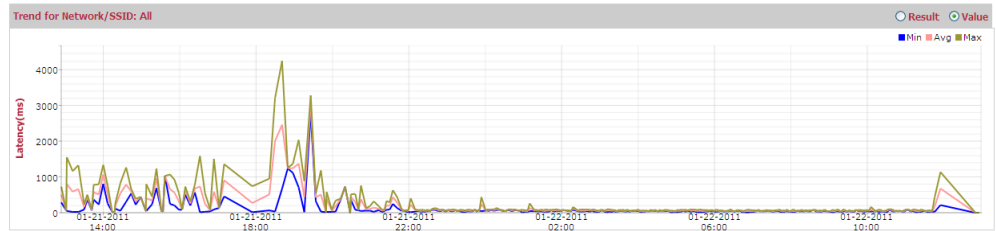
Two buttons are available in the *Value Graph* section. They are as follows:

- Latency
- Packet Loss




The respective graphs are displayed as per the selection of the respective option as mentioned above.

Figure 133 on page 362 illustrates the Results Trend Value graph screen.

Figure 133: Results Trend - Value Graph



The *Date/Time*, *Minimum*, *Average* and *Maximum* numbers are displayed with three different colors as follows:

Result Type	Description	Color
Minimum	The <i>Minimum</i> value is calculated by comparing all the values in the each of the test examples and the least value is considered as the minimum value.	
Average	The <i>Average</i> value is the sum of all the values in each of the test examples, divided the total by the number of values.	
Maximum	The <i>Maximum</i> value is calculated by comparing all the values in each of the test examples and the highest value is considered as the maximum value.	

For Example:

Consider the three sample *Throughput TCP* completed results (Test1, Test 2 and Test 3) with their test details. Each test consists of 2 Rows and 2 columns of data, since we have 2 ESS Profiles and 2 AP-Radios:

Test 1			Test 2			Test 3		
IF ID \ ESS Profile	kkp	kkp clear	IF ID \ ESS Profile	kkp	kkp clear	IF ID \ ESS Profile	kkp	kkp clear
AP-1-1	2.7 Mbps	23.7 Mbps	AP-1-1	2.0 Mbps	21.2 Mbps	AP-1-1	2.7 Mbps	16.7 Mbps
AP-1-2	9.7 Mbps	70.1 Mbps	AP-1-2	8.4 Mbps	67.7 Mbps	AP-1-2	10.2 Mbps	66.4 Mbps
AP-2-1	1.8 Mbps	15.8 Mbps	AP-2-1	1.6 Mbps	22.7 Mbps	AP-2-1	2.0 Mbps	19.2 Mbps
AP-2-2	9.2 Mbps	67.7 Mbps	AP-2-2	10.0 Mbps	68.5 Mbps	AP-2-2	10.1 Mbps	68.6 Mbps

From the above mentioned three completed throughput test results (Test1, Test 2 and Test 3), the number of *Minimum*, *Average* and *Maximum* values can be calculated as follows:

- **Minimum:**
The *Minimum* value is calculated by comparing all the values in the each of the test exam-

ples and the least value is considered as the minimum value. The minimum value calculated is 1.6 Mbps.

- **Maximum:**
The *Maximum* value is calculated by comparing all the values in each of the test examples and the highest value is considered as the maximum value. The maximum value calculated is 70.1 Mbps.
- **Average:**
The *Average* value is the sum of all the values in each of the test examples, divided by the total number of values.

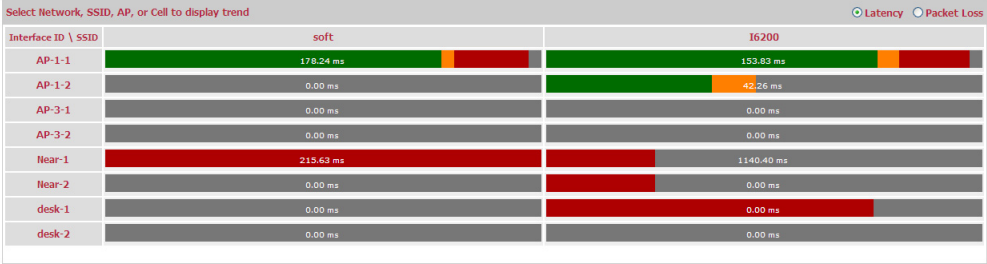
Test	Minimum	Average	Maximum
Test 1	1.8 Mbps	25.08 Mbps	70.1 Mbps
Test 2	1.6 Mbps	25.26 Mbps	68.5 Mbps
Test 3	2.0 Mbps	24.48 Mbps	68.6 Mbps

Matrix Section

The *Matrix* of the test instances consists of bar charts for table cells, average test instance value across the results.

Figure 134 on page 363 illustrates the *Matrix* section of the *Results Trend* screen.

Figure 134: Results Trend - Matrix Section



For Example:

Test 1			Test 2			Test 3		
IF ID \ ESS Profile	kkp	kkp clear	IF ID \ ESS Profile	kkp	kkp clear	IF ID \ ESS Profile	kkp	kkp clear
AP-1-1	2.7 Mbps	23.7 Mbps	AP-1-1	2.0 Mbps	21.2 Mbps	AP-1-1	2.7 Mbps	15.7 Mbps
AP-1-2	9.7 Mbps	70.1 Mbps	AP-1-2	8.4 Mbps	67.7 Mbps	AP-1-2	10.2 Mbps	66.4 Mbps
AP-2-1	1.8 Mbps	15.8 Mbps	AP-2-1	1.6 Mbps	22.7 Mbps	AP-2-1	2.0 Mbps	19.2 Mbps
AP-2-2	9.2 Mbps	67.7 Mbps	AP-2-2	10.0 Mbps	68.5 Mbps	AP-2-2	10.1 Mbps	68.6 Mbps

Consider the above three completed throughput test results (Test1, Test 2 and Test 3). Each test consists of 2 Rows and 2 columns of data, since we have 2 ESS Profiles and 2 AP-Radios. From the above mentioned Test 1, Test 2 and Test 3, the *Minimum*, *Average* and *Maximum* values can be calculated as follows:

- **Minimum:**
Consider the first row and first column of AP-1-1 in all the three tests. The *Minimum* value is calculated by comparing the values in the First row of AP-1-1 in all the three tests. The minimum value calculated is 2.0 Mbps.
- **Maximum:**
Consider the first row and first column of AP-1-1 in all the three tests. The *Maximum* value is calculated by comparing the values in the First row of AP-1-1 in all the three tests. The maximum value calculated is 2.7 Mbps.
- **Average:**
Consider the first row and first column of AP-1-1 in all the three tests. The *Average* value is the sum of the values in the First row of AP-1-1 in all the three tests, and divided the total by three. The average value calculated is 2.4 Mbps ($2.7+2.7+2.0 = 7.4 / 3 = 2.4$).

The below table summarizes the *Minimum*, *Maximum*, *Average* and *Test Count* values for the first row and first column of AP-1-1 and the second row and second column of AP-1-2.

IF ID \ ESS Profile	kkp				kkp_clear			
AP-1-1	Minimum	Maximum	Average	Test Count	Minimum	Maximum	Average	Test Count
	2.0 Mbps	2.7 Mbps	2.46 Mbps	3	16.7 Mbps	23.7 Mbps	20.53 Mbps	3
AP-1-2	Minimum	Maximum	Average	Test Count	Minimum	Maximum	Average	Test Count
	8.4 Mbps	10.2 Mbps	9.43 Mbps	3	66.4 Mbps	70.1 Mbps	68.0 Mbps	3

The below table provides the values in *Percentage (%)*, for the first row and first column of AP-1-1 and the second row and second column of AP-1-2.

IF ID \ ESS Profile	kkp				kkp_clear			
AP-1-1	Good	Fair	Bad	Incomplete	Good	Fair	Bad	Incomplete
	66.6%	33.3%	0%	0%	66.6%	33.3%	0%	0%
AP-1-2	Good	Fair	Bad	Incomplete	Good	Fair	Bad	Incomplete
	100%	0%	0%	0%	100%	0%	0%	0%



The test results for *Connectivity*, *Voice* and *Throughput UDP Test Types* are displayed in% (percentage) for *Packet Loss* and ms (Millisecond) for *Latency* or average round trip times (rtt). The test result for *Throughput UDP* is displayed in Mbps,% (percentage) for *Packet Loss* and ms (Milli Second) for *Latency*.

Failure Trends

1. Navigate to *Monitor > Trends > Failure Trends*. The *Failure Trends* screen provides the graphical representation of the failed recurring tests.
2. This page is divided into the following three sections:
 - “*Header Section*” on page 365
 - “*Failure Trends Graphs Section*” on page 366
 - “*Matrix Section*” on page 368

Header Section

The header section consists of the following fields as displayed in the below table:

Field	Description
Controller Name	Displays the complete list of <i>Controller Names</i> , for which the test was run. You can either select the <i>Controller Name</i> or the <i>Controller IP</i> . By the selection of either of the options, the other is selected automatically.
Controller IP	Displays the complete list of <i>Controller IPs</i> for which the test was run. You can either select the <i>Controller IP</i> or the <i>Controller Name</i> . By the selection of either of the options, the other is selected automatically.
Test Type	<p>Displays the Test Type as follows:</p> <ul style="list-style-type: none"> • Connectivity: <i>Connectivity</i> describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another. The test result for <i>Connectivity</i> is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt). • Throughput: <i>Throughput</i> is the amount of data moved successfully from one place to another in a given time period. The throughput test type can further be divided as follows: <ul style="list-style-type: none"> • Throughput TCP: The test result for <i>Throughput TCP</i> is displayed in <i>Mbps</i>. • Throughput UDP: The test result for <i>Throughput UDP</i> is displayed in <i>Mbps</i>, % (percentage) for <i>Packet Loss</i> and <i>ms</i> (Millisecond) for <i>Latency</i>. • Voice: <i>Voice</i> is simulated using multiple thread of ping traffic. The selection of the <i>Test Type</i> as <i>Voice</i> determines the rest of the options on the page. The test result for <i>Voice</i> is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt). <p>Note: The <i>Connectivity</i>, <i>Voice</i>, and <i>Throughput UDP</i> test type allows you to choose a type of <i>Matrix</i> from the <i>Matrix</i> section. The types are Latency and Packet loss.</p> <p>Select one of the above mentioned Test Type from the drop-down list.</p>

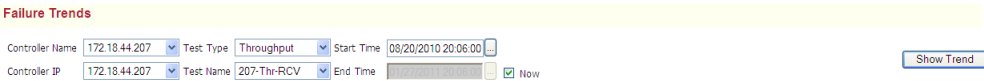
Field	Description
Test Name	Displays the <i>Test Name</i> . Select the test name from the drop-down list.
Start Time	Select the <i>Start Time</i> . The format followed is the <i>mm/dd/yyyy</i> and <i>hh:mm:ss format</i> . The time can be entered manually or by selecting the calendar icon. The calendar is displayed, where the date and time can be modified manually.
End Time	The <i>End Time</i> is automatically selected for the current date. To modify the end time and date, uncheck the <i>Now</i> option and enter the date manually. Else select the calendar icon. The calendar is displayed, where the date and time can be modified manually.

1. Select all the parameters from the above mentioned fields.
2. Select the *Show Trend* button. The *FCA (Failure Causal Analysis)* graph results are displayed.

Figure 135 on page 366 illustrates the *Failure Trend* header section.

The charts can be modified according to the selected row or column or single cell or for all the table cells.

Figure 135: Failure Trends - Header Section

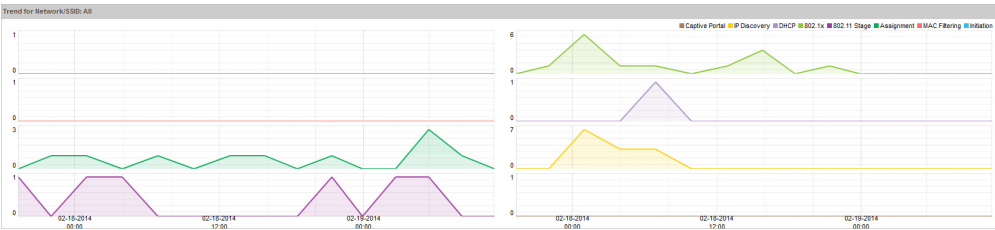


Failure Trends Graphs Section









The *Failure Trend Graph* section displays the details of the *Eight* varieties of failure cases. The individual data for each of the stages is plotted in an individual graph. The details can be viewed by hovering the mouse pointer over each graph. The values for each of the stage is displayed with different colors.

Figure 136 on page 366 illustrates the *Failure Trend* graph screen.

Figure 136: Failure Causal Analysis graph



The *FCA (Failure Causal Analysis)* provides details for the failure cases. The following are the eight failed stages:

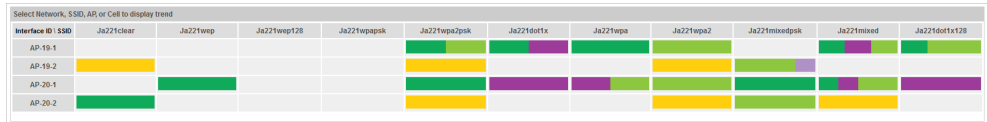
Result Type	Description	Color
Initiation	Here, <i>SAM</i> gathers the data that requires to start a test and initiates the test. If <i>SAM</i> fails to gather the data or failed to start a test, <i>SAM</i> says the test has failed in this stage.	
MAC Filtering	The station goes through this stage when MAC filtering is enabled. A MAC filtering is either ACL-based or Radius-based. If the authentication of MAC filtering succeeds, the station proceeds to the next stage assignment. If MAC filtering is disabled, this stage is skipped.	
Assignment	Here, the station is assigned to an AP (BSSID). If the station fails to get an assignment from the AP, <i>SAM</i> says assignment has failed or not reached.	
802.11 Stage	Here, the station will be authenticated and associated to an AP (BSSID).	
802.1xAuth	This is for <i>Radius-based User authentication</i> and for Key exchange. The station goes through this stage only for radius based profiles. If the radius authentication fails or key exchanges are timed out, <i>SAM</i> says 802.1x failed. This also includes EAP failures which include wpa-psk and wpa2psk along with Radius failures.	
DHCP	Here, the station tries to get an IP address using DHCP mechanism. If the station receives the IP address, this stage is successful, else <i>SAM</i> treats this stage as failed.	
IP Discovery	Once the station receives an IP address using static or DHCP mechanism, this will be updated to the controller. After the controller receives this update the stage is passed. If captive portal is not enabled for connected profiles, the station is successfully connected to the network. If the controller does not get update this stage is failed.	
Captive Portal	The station goes through this stage only if the captive portal is enabled for connected profile. The station does a captive portal Authentication. Once the captive portal authentication is successful, the stage is passed and the client clears all the stages successfully and is connected to the network.	

Matrix Section

The *Matrix Section* of the test instances consists of bar graph depicting the failure count graphically. The values of each of the eight failed stages can be viewed by hovering the mouse pointer over the section.

[Figure 137 on page 368](#) illustrates the *Matrix* section of the *Failure Trend* graph screen.

Figure 137: Matrix section



Monitor Tests

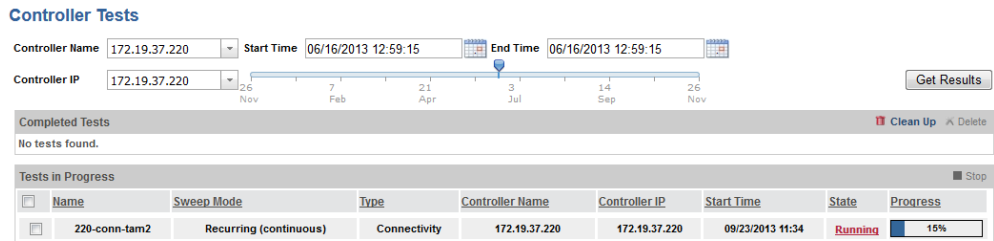
The *Tests* in the *Monitor* menu allows you to monitor the *completed*, *ongoing baseline* and *scheduled tests*.

View Test Results for a Controller

To view The test result for a controller during the given time period, follow these steps:

1. Navigate to *Monitor > Tests > Controller Tests*.
See [Figure 138 on page 368](#) illustrates the *Controller Tests* screen.

Figure 138: Controller Tests



2. Select a *controller name* or *IP address* from the drop-down list.
3. The controller list, displays all the controllers for which the test was run in the past and for which the tests that are in progress.
4. Select the *Start Time* and *End Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss* format. The time can be entered manually or by selecting the *calendar* icon. The calendar is displayed, where the date and time can manually be modified.

5. The *Start Time* and *End Time* can also be modified by adjusting the slider. The slider can be dragged along a fixed-length line representing a linear range dates.



The *Start Time* to *End Time* duration cannot exceed more than one week.

6. Select *Get Results*. The completed test results for the selected controller is displayed. The controller results for the tests that are in progress is also displayed.
7. Select on the result of a test (*Good, Bad, Fair, Failed in the Result* column). Click *Close*.

View a Test in Progress

1. Navigate to *Monitor > Tests > Ongoing Tests*.
See [Figure 139 on page 369](#) illustrates the *Ongoing Tests* screen.

Figure 139: Ongoing Tests

Ongoing Tests

Tests in Progress								Stop
<input type="checkbox"/>	Name	Sweep Mode	Type	Controller Name	Controller IP	Start Time	State	Progress
<input type="checkbox"/>	220-conn-tam2	Recurring (continuous)	Connectivity	172.19.37.220	172.19.37.220	09/23/2013 11:34	Running	34%

2. The *Ongoing Tests* screen lists all the *scheduled* and *baseline* tests that are still in progress. A test is selected by checking the boxes. A test, in a run or wait state can be stopped by clicking *Stop*. If the test in a run state is stopped, the state is modified from *run* to *stop*.
3. The *Tests in Progress* table in the *Ongoing Tests* screen display the *Name, Sweep Mode, Type, Controller Name, Controller IP, Start Time, State and Progress* of the *ongoing scheduled and baseline* tests.

See the **Ongoing Tests** screen (*Monitor > Tests > Ongoing Tests*) in Online Help for detailed information on *Ongoing Tests* topic.

View all the Completed Tests

You can view The test result for a selected controller during a given time period, or you can view most recent scheduled *Throughput/ Connectivity/ Voice* test results from *FortiWLM* during a given time period. To view most recent test results from *FortiWLM* during a given time period, follow these steps:

1. Navigate to *Monitor > Tests > Completed Tests*
2. Select the test result **Good, Bad, Fair, Failed** in the *Result* column.
The detailed test results are displayed.

Definitions of Test Results

The result of a successful test can be *good*, *bad*, or *fair*. The amount of change is configured with the good-threshold and bad-threshold parameters you provided when you created the test (see [“Add a Scheduled Test” on page 333](#)).

Result	What it means
Good	If the number of tests with fair and bad results is zero, then a test is good.
Bad	If there is at least one test with a bad result, then a test is bad. Click the number in this column to see the results of the bad tests.
Fair	If no test has a bad result and at least one test has a fair result, then a test is fair.
Controller Offline	The Controller is offline.
Stopped	The test was stopped.
No Baseline	No baseline (connectivity or throughput) was available for comparison on this controller. This can happen, for example, if you add new access points after the running the last baseline for this controller.

Click *Result* in the *Actions* column to see a list of tests performed over each radio and SSID. To see results for each test, click the cell of the table in the *Actions* popup.

12 Reporting and Notification in SAM

In *Reports* page, one-time reports can be generated by following these steps:

1. Navigate to *Reports & Notify > Reports > Instant Reports*.
2. Select a *Report Type* from the drop-down list. The following are the types of report displayed in the list.
 - Tests Report
 - Trends Report
3. Select the *Controller Name* or the *Hostname* from the drop-down list. By selecting the *Controller Name*, the *Controller IP* is auto selected and vice versa.
4. Select the *Start Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss* format. The time can be entered manually or by clicking the calendar icon. The calendar is displayed, where the date and time can manually be modified.
5. The *End Time* is automatically selected for the current date. To modify the *End Time* and *Date*, uncheck the *Now* option and enter manually. Else click the calendar icon. The calendar is displayed, where the date and time can manually be modified.
6. Click *Show Results* button.
7. A list of completed test, that falls in the selected time durations appears on the same screen with the fields as displayed in the below table:






The below mentioned fields are displayed only for the Report Type - Tests report.

For the Report Type - Trends Report, the Controller Name and the Controller IP are displayed.

Field	Description
Name	Displays the name of the report.
Type	Displays a test type.
Controller Name	Displays the name of the controller.
Start Time	Displays the start time of the test.
Controller IP	Displays the IP address of the controller.
Start Time	Displays the start time.

Field	Description
End Time	Displays the end time of the test.
Result	Displays the type of result. If <i>Good</i> , <i>Fair</i> , <i>Bad</i> , <i>Controller Offline</i> , <i>No Neighbors</i> , <i>Stopped</i> or <i>Config Retrieval Failed</i> .
Good	Displays the number of <i>Good</i> test type of result. If the number of tests with fair and bad results is zero, then a test is <i>Good</i> .
Fair	Displays the number of <i>Fair</i> test type of result. If no test has a bad result and at least one test has a fair result, then a test is fair.
Bad	Displays the number of <i>Bad</i> test type of result. If there is at least one test with a bad result, then a test is bad.
Controller Offline	Displays the number of controller offline type of result. If the server is unable to reach the controller while starting a test, the controller offline message is displayed in the results section.
No Neighbors	Displays the number of no neighbors type of result. If there are <i>No APs</i> or if all the APs in the controller looks offline or not reachable, then the no neighbors message is displayed in the results section.
Stopped	Displays the number of <i>Stopped</i> types of result. If you stop a running test, the output is displayed as <i>Stopped</i> . Clicking on this will display the test details of the percentage completed.
Config retrieval failed	Displays the number of config retrieval failed type of result. If, for some reason the test starts and we are unable to retrieve any configuration, the config retrieval failed is displayed in the results section.

8. To generate a report, select a test and click on the *Generate Report* button.
9. Multiple tests can be selected and reports can be generated. The Report is generated and can be saved in the following formats.

Name of the Format	Icon	Explanation
Save HTML Report		Click the <i>HTML</i> icon to export and save the report to <i>HTML</i> format.
Save Pdf Report		Click the <i>Pdf</i> icon to export and save the report to <i>Pdf</i> format.
Save Excel Report		Click the <i>Excel</i> icon to export and save the report to <i>Excel</i> format.

10. The report can also be emailed by clicking the  Icon and notification profile.

11. Click the  Icon to print the report.

PCI Compliance

FortiWLM can be validated against specific PCI requirement compliances.

- To run a compliance test, set Run PCI test to **Yes**.
- Now select the tests to validate FortiWLM and click the **RUN TEST** button (located at the bottom of the page). After the test is executed, an alert box displays the status of the test.
- The page is refreshed to show the list of PCI requirements that are validated for FortiWLM. The validation results are shown in GREEN ticks if they are passed and in RED CROSS circle if the compliance is not validated or failed.
- Click the **DOWNLOAD PDF REPORT** button to get a copy of the validation results in PDF format.

Notification

Add a Notification Filter in SAM

A notification filter defines the conditions that trigger an email. When you create a notification filter you also name a notification profile. When the notification filter is triggered, it sends a message to the list of recipients in the notification profile. Configure a notification filter in SAM by following these steps:

1. Navigate to *Service Assurance > Reports & Notify > Notify > Notification > Add*.
Figure 140 on page 374 illustrates the *Add Notification Filter* screen.

Figure 140: Add Notification Filter

2. In *Add Notification Filter* screen, provide the following information as mentioned in the below table:

Field	Explanation
Name	Provide the test name. The test name can be from 1 - 31 characters long, including letters, numbers, and special characters.
Test Type	Select the test type from the drop-down list. This field is either <i>All</i> , <i>Throughput</i> , <i>Connectivity</i> or <i>Voice</i> .
Controller Name	Select controller name from the drop-down list. The list includes all the controller names mapped to the <i>FortiWLM</i> inventory.
Controller IP	Select controller IP from the drop-down list. The list includes all the controller names mapped to the <i>FortiWLM</i> inventory.
Status	<i>Enabled</i> is the default option. Select <i>Disable</i> to deactivate this filter; then it will not monitor the controller.
Interval	Select the time Interval. The interval options is <i>Daily</i> and <i>Weekly</i> .

Field	Explanation
Start Time	Select the <i>Start Time</i> . The format followed is the <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format. The time can be entered manually or by clicking the calendar icon. The calendar is displayed, where the date and time can manually be modified.
Mode	Select the notification mode from the drop-down list. The notification mode determines how many times the message is sent to the email recipients listed in the profile. The options are as follows: <ul style="list-style-type: none"> • One Time: This option enables you to send the email once when the trigger incident occurs and then delete the entry from the notification list. • Recurring: This option enables you to keep sending emails at the configured date and time every week, until the profile is disabled.
Notification Profile	Select the notification profile from the drop-down list. Notification profiles display a list of emails configured in the <i>Forti-WLM</i> application. Indicate a profile here; all email addresses in the profile will be sent the <i>Notification Message</i> indicated below.
Notification Message	Provide a subject or notification message up to 64 characters long.

3. Click *Save*.
4. The *Notification Filter* is added and displayed on the *Notification Filters* screen.

Edit Notification Filters

Edit a Notification Filter by following these steps:

1. Navigate to *Configure > Infrastructure > Notification*.
2. Select a notification filter and click the *Edit* icon that corresponds to the filter.
3. Modify the fields.
4. Click *Save*.

Delete Notification Filters

Delete a Notification Filter by following these steps:

1. Navigate to *Configure > Infrastructure > Notification*.
2. Select a notification filter and click the *Delete* icon that corresponds to the filter. A confirmation message for deletion is displayed.
3. Click *OK*.

4. Click *Refresh*. The filter is removed from the drop-down list.

13 SAM Administration

Maintenance

In SAM all the *Baseline* and *Scheduled* sweeps are configured to run continuously (once, instant, hourly, daily, and weekly sweeps). The results of the sweeps are stored in the database and may occupy enormous space. To prevent accumulation of older data, you can schedule a regular cleanup activity from the *Maintenance* page in SAM.

To access the *Maintenance* screen on SAM:

1. Navigate to *Service Assurance > Administration > Maintenance*.

Figure 141 on page 377 illustrates the *Maintenance* screen.

Figure 141: Maintenance

Maintenance

Database cleanup schedule: Weekly, 00:00 AM, (12Hr 24Hr)
Sunday
Cleanup Tests older than*: 90 Valid range: [30-365 days]

2. On the *Maintenance* screen, select the following fields:
 - *Database cleanup schedule*: Select the database cleanup schedule from the drop-down list. Following are the options:
 - *No Schedule*: This is the default field. Here the database cleanup schedule is not configured.
 - *Daily*: The daily option allows you to select the time and time format (12 Hr or 24 Hr).
 - *Weekly*: The weekly option allows you to select,
 - the time from the drop-down list,
 - the time format (12 Hr or 24 Hr) and
 - the day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday) from the drop-down list.
 - *Cleanup Tests older than*: This option allows you to enter the number of days. The data older than the number of days entered will be deleted.

- *For Example:* Enter the value as 30 in the *Cleanup Tests older than the field*. The data older than 30 days is deleted from the scheduled time. The valid range provided is [30-365 days].
- 3. Select *OK* to accept all the changes performed on the *Maintenance* screen.
- 4. Select *Refresh* to view the changes performed.

Licensing in SAM

The *Licensing* for the *Service Assurance Manager* is performed in the *FortiWLM*. The procedure for procuring and uploading the license is similar in all 3 products (*NM*, *SAM*, and *SM*). The licenses procured are displayed in the *License Usage Summary* section of *FortiWLM*.

License Usage Summary

The *License Usage Summary* section provides a graphical representation of the License usage for *EZRF-NM-VISUALIZE*, *EzRF-NM-BASE*, *SAM* and *Spectrum Manager*. The following varieties of graphs with different colors are represented:

- **License Consumed** - The number of licenses used. This is represented in yellow color.
- **Available licenses** - The number of licenses available which remains unused. This is represented in green color.
- **Unlicensed** - The number of licenses which are Unlicensed. This is represented in red color.

See "[FortiWLM Licensing](#)" on page 299.

Although, the license for *SAM* is procured and uploaded in the *FortiWLM* application, the applying of the license is performed in *SAM*.



The *License Management* for *SAM* 2.0 installed on *FortiWLM* 3.0, is handled by *FortiWLM* 3.0. Uploading or validating the license is handled by the *FortiWLM*.

The *License Management* link will no more be available for *SAM* 2.0 when installed on the *FortiWLM* 3.0 and above.

Apply License

1. Navigate to *Service Assurance > Administration > License Manager*.

Figure 142 on page 379 illustrates the *License Manager* screen.

Figure 142: License Manager

License Manager
Total Licenses: 50, Used Licenses: 11, Available Licenses: 39

<input type="checkbox"/>	Serial Number	AP Name	Controller Name	Controller IP	Availability Status	License Status
<input type="checkbox"/>	00:0c:a6:0a:11:59					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:55					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:53					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:56					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:45					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:5f					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:af					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:b7					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:09					Licensed
<input type="checkbox"/>	00:0c:a6:0a:12:06					Licensed
<input type="checkbox"/>	00:0c:a6:0a:11:77					Licensed

2. The *License Manager* screen displays the following details:
 - **Total Licenses:** Displays the total number of licenses allocated. This includes the sum of both *Used* and *Available* licenses.
 - **Used Licenses:** Displays the number of used licenses.
 - **Available Licenses:** Displays the number of available licenses.
3. It also displays a table of unlicensed APs, as listed below:

Field	Description
Serial Number	Displays the <i>MAC address</i> of the AP.
AP Name	Displays the <i>AP Name</i> .
Controller Name	Displays the <i>IP address</i> or the name of the controller.
Controller IP	Displays the <i>IP address</i> of the controller.
License	Displays the <i>License Status</i> of the controller. The following are the types: <ul style="list-style-type: none"> • Licensed • Unlicensed

4. The unlicensed APs can be licensed by following the below mentioned steps:
 - Select the unlicensed APs from the table by clicking the check box.
 - Select *Add to License* option. A confirmation message is displayed notifying that APs once added to the license can't be removed.
 - Select *OK* to proceed. The MAC addresses of the selected APs are added to the data-base.
 - Select *Refresh* option to view the changes performed.

Remove License

The *Remove License* option allows you to remove *offline APs* and *unknown APs* (APs that are not present in Inventory table) by following the below mentioned steps:

1. Select the unlicensed APs from the table by clicking the check boxes.
2. Select *Remove License* option.
3. A confirmation message is displayed notifying the removal of APs.
4. Select *OK* to proceed. The selected APs are deleted from the database.
5. Select *Refresh* option to view the changes performed.

14 Getting Started Spectrum Manager

Sensors Setup

To setup Sensors, the following basic setup must be performed:

1. **Controller Hardware:** Ensure to select one of the following types of *Controller Hardware* from the below list:
 - MC1550
 - MC3200
 - MC4200
 - FortiWLC-50D
 - FortiWLC-200D
 - FortiWLC-500D
 - FortiWLC-1000D
 - FortiWLC-3000D
1. **Controller VM:** Ensure to select one of the following types of *Controller VM* from the below list:
 - MC1550V
 - MC3200V
 - MC4200V
 - FWC- VM-50
 - FWC –VM-200
 - FWC –VM-500
 - FWC –VM-1000
 - FWC-VM-3000
2. **Controller Software:** The *Controller Software* must be of the latest version.
3. **Sensors Hardware:**

The Sensors operate like Access Points and appears in the list of the Access Points. Sensors must be connected using L3.

After performing the basic setup, the connected sensors must be validated. To validate the online sensors, the following *Controller CLI* commands must be typed.

```
Spectrum-Manager# sh ap
```

AP ID	AP Name	Serial Number	Uptime	Operation State	Availability	Runtime	Connectivity	IP Address	AP Model
1	AP-1	00:0c:e6:0a:5c:1d	01d:18h:42m:56s	Enabled	Online	6.0-1-0	L3	172.19.32.77	AP433is
2	AP-2	00:0c:e6:0e:23:83	01d:18h:35m:18s	Enabled	Online	6.0-1-0	L3	172.19.32.56	AP1014i
3	AP-3	00:0c:e6:07:d5:b5	01d:18h:42m:53s	Enabled	Online	6.0-1-0	L3	172.19.32.197	PSM3x
4	AP-4	00:0c:e6:0a:10:3e	01d:18h:40m:08s	Enabled	Online	6.0-1-0	L3	172.19.32.115	AP1010e

AP Table(4 entries)

The *Sensors* must be added to the *FortiWLM* server, to monitor the interference in *Spectrum Manager*. The section provides details to add *Sensors* to the *FortiWLM* server.

Add Sensors to FortiWLM

The sensors are available on the controller and the selected controller is added to the *NM* server. To add the controllers onto *NM* server, follow the below steps:

1. Navigate to *FortiWLM > Inventory > Controllers* displaying the *Controllers* screen. The *Controllers* screen appears empty; hence the controllers must be added.
2. To add the Controllers, select *Add* on the *Controllers* screen.
3. In the *Controllers-Add* screen provide the following details:
 - **Hostname/IP Address:** Type the controller's IP address or name.
 - **SSH Port:** Type the SSH port number. The controller can be added to the user defined port number.
 - **User:** Type a user ID for the controller.
 - **Password:** Type an encrypted password for the controller.
 - **Controller Group Name:** Select a controller group name from the drop-down list. Controllers mapped to NM can be grouped.
 - **Server Connectivity Preference:** Select the *Server Connectivity Preference*. The options are as follows:
 - **User Default:** This option is selected if the controller is in the same sub-network (Not behind NAT).

- **User Server Public IP:** This option is selected to configure the public *IP Address* in *Administration->Server Details->Public IP Address* screen.
- **Specify Address:** This option is selected if the controller is behind NAT. The server IP address, which is reachable from the controller, must be specified in the *Server IP Address* field.
- **VPN Server IP Address:** This option is selected
- **Server IP Address:** Type the Server IP Address. This option is enabled, only if you want to specify an IP address by selecting the *Specify Address* check box in the *Server Connectivity Preference*.
- 4. Select *Save*. The new controller is included and displayed on the *Controllers* screen. The new controllers *Availability State* appears *Offline* until it is discovered.
- 5. The discovered controller displays the complete details with the *Availability State* appearing as *Online*.
- 6. Select the *Edit* option of the discovered *Controller*.
- 7. In the *Controller Inventory Details - Update* screen, select the *Access Points* tab. The Sensors and APs, associated with the discovered controller are listed here.
- 8. The *Controller* is now added in the *FortiWLM* server. Ensure the following credentials are displayed from the *FortiWLM* side:
 - Controller MAC address
 - Controller Software Version
 - Controller Status

Add Sensors to Map Management

The sensors added through the *Controller Inventory* screen must be included on the *Visualization Map Management* screen. This helps to locate APs and visualize the interference of the APs on the floor.

Maps must accurately represent the physical layout of the site and be as close to scale as possible. We suggest using a separate map for each floor in multi-level buildings and images based on accurate architectural drawings. Crop the map of each floor to remove any extra space and save it as a *PNG, JPEG, BMP, or GIF* file, no larger than 2MB.

There are multiple tasks required to set up a working map:

- Import a graphic map of the floor
- Add a new campus to FortiWLM
- Add a building
- Add a floor
- Place AP icons on the map to depict the WLAN network topology.
- View the map

See the *Map Management* screen (*Visualization > Map Management*) in the *NM* Online Help for detailed information on *Map Management* topic.

15 Wireless Intrusions Prevention System (WIPS)

Fortinet's WIPS provides complete wireless threat detection and mitigation into the wireless network infrastructure. It detects wireless intrusions using predefined and custom signatures on an integrated platform with other WLAN management applications.

For more information, see the *Wireless Intrusion Prevention System (WIPS) User Guide*.

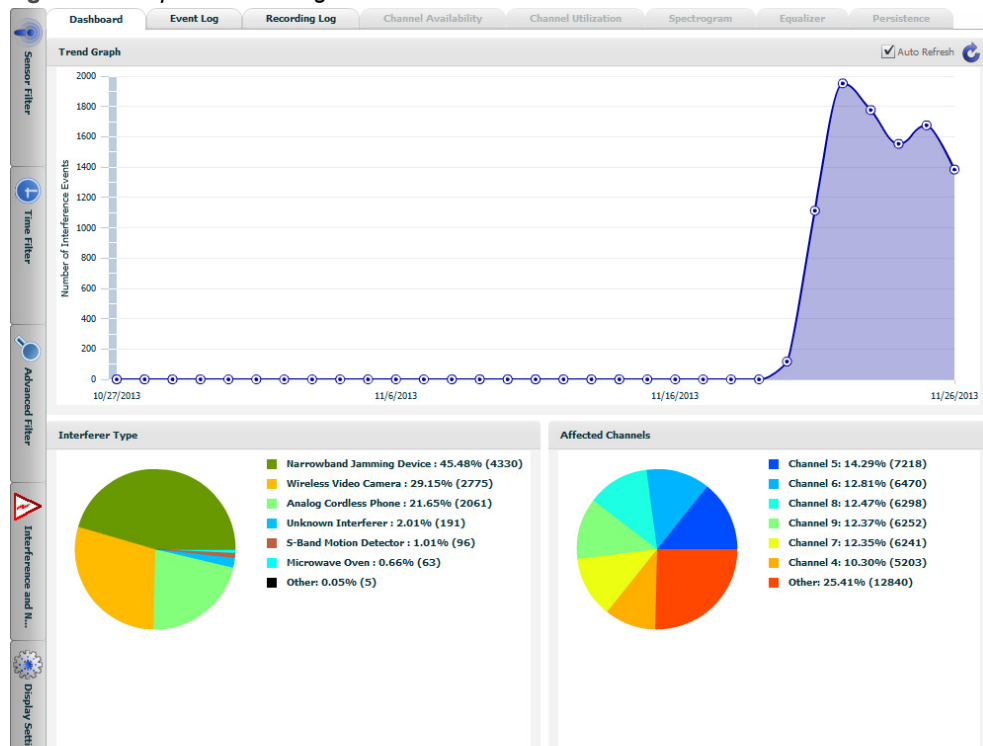
16 Monitoring Spectrum Manager

Spectrum Manager Dashboard

The *Spectrum Manager Dashboard* screen presents the interference information gathered from various “*Sensors*” on page 412 (“*Software Sensors*” on page 412 and “*Hardware Sensors*” on page 412). It provides a graphical representation of the Interference devices activity in the 2.4Ghz and 5Ghz spectrum.

Figure 143 on page 387 illustrates the *Spectrum Manager Dashboard* screen.

Figure 143: *Spectrum Manager Dashboard*



If the *Dashboard* screen is empty without *Graphs* and *Events*, ensure the *Controller time* and *FortiWLM time* are in sync.

The following table depicts the various sections displayed on the *Dashboard* screen.

Trend Graph	The <i>Trend Graph</i> plots the number of interference events observed over a period of time.
Interferer Type	The <i>Interferer Type Graph</i> is a pie chart divided by the different types of interferer observed in the set duration. The area of each sector is proportional to the percentage of the number of individual interference events from a particular type of interferer against the total number of interference events in the set duration.
Affected Channels	<p>The <i>Affected Channels Graph</i> is a pie chart that plots the number of times, a particular channel was impacted due to an interference events. The area of each sector is proportional to the percentage of the number of events that impacted a particular channel against the total number of events.</p> <p>Note: An interference event impacts multiple channels simultaneously.</p>

The *Dashboard* screen provides various expandable control panels to filter database and modify display settings. For further information, refer to [“Control Panels” on page 399](#) topic.

The *Dashboard* screen allows you to connect to the following other tabs:

1. [“Event Log” on page 389](#)
2. [“Spectrum Manager - Recording Log” on page 391](#)
3. [“Spectrum Manager - Channel Availability” on page 394](#)
4. [“Spectrum Manager - Channel Utilization” on page 395](#)
5. [“Spectrum Manager - Spectrogram” on page 396](#)
6. [“Spectrum Manager - Equalizer” on page 396](#)
7. [“Spectrum Manager - Persistence” on page 397](#)



The above mentioned tabs from 3 to 7 are enabled only, by selecting the *View live data from sensor* option on the *Event Log* screen or it can be viewed through *Show Spectrum Display* of the selected sensor displayed on the Sensor's page. For further information, refer to *Spectrum Manager - Event Log* screen.

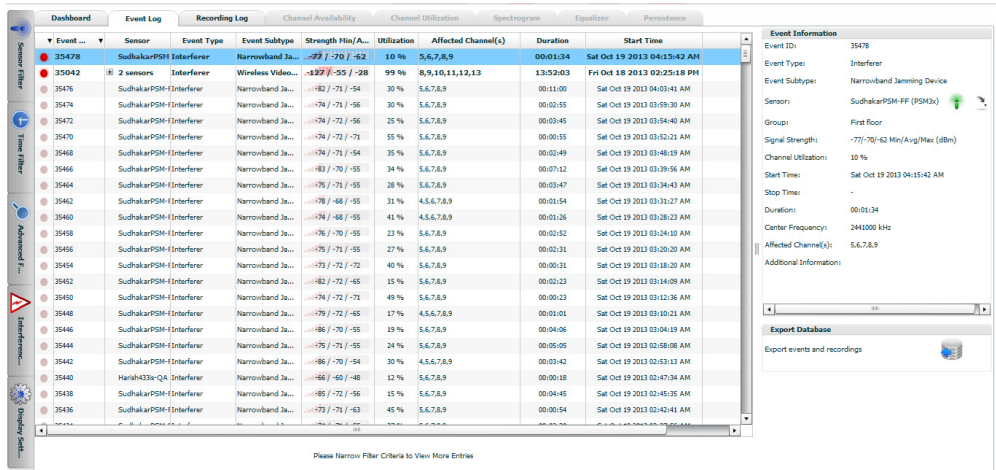
Event Log

Spectrum Manager > Monitor > Dashboard > Event Log

The *Spectrum Manager Event Log* screen provides the detailed log information of the sensors.

Figure 144 on page 389 illustrates the *Spectrum Manager Event Log* screen.

Figure 144: *Spectrum Manager - Event Log*



The following table depicts the *Event Information* displayed on the *Event Log* screen:

Field	Description
Event ID	Displays the <i>Event ID</i> .
Event Type	Displays the type of Event.
Event Subtype	Displays the interference source name.

Field	Description
Sensor	<p>Displays the name of the selected <i>Sensor</i>. The following options are available for selection:</p> <ul style="list-style-type: none"> • <i>View live data from sensor</i>: This option allows you to read the <i>live data from the Sensor</i>. <p>The below mentioned tabs are enabled by the selection of the <i>View live data from sensor</i> option.</p> <ul style="list-style-type: none"> • Channel Availability • Channel Utilization • Spectrogram • Equalizer • Persistence <p>The above mentioned tabs reveal data of the selected <i>Sensor</i> in their respective tabs.</p> <ul style="list-style-type: none"> • <i>Show interferer on map</i>: Select the <i>icon</i> <p>The <i>E(z)RF Map Management</i> screen is displayed, depicting the location of the interfering device on the Floor.</p>
Group	Displays the sensor's group.
Signal Strength	Displays the <i>Signal Strength</i> of Interference with <i>Min, Max, and Avg</i> values in dBm.
Channel Utilization	Displays the percentage of channel utilized by the interferer.
Start Time	Displays the <i>Start Time</i> of the interference detected by the sensor.
Stop Time	Displays the <i>Stop Time</i> of the interference detected by the sensor.
Duration	Displays the <i>Duration</i> of the interference detected by the sensor.
Center Frequency	Displays the <i>Center Frequency</i> of the interference.
Affected Channel(s)	Displays the number of channels affected by the interference.
Recording Id	Displays the recording event Id.
Additional Information	Displays the interfere type for alert triggered event.
Active	Displays the number of active events highlighted with bold red dot.

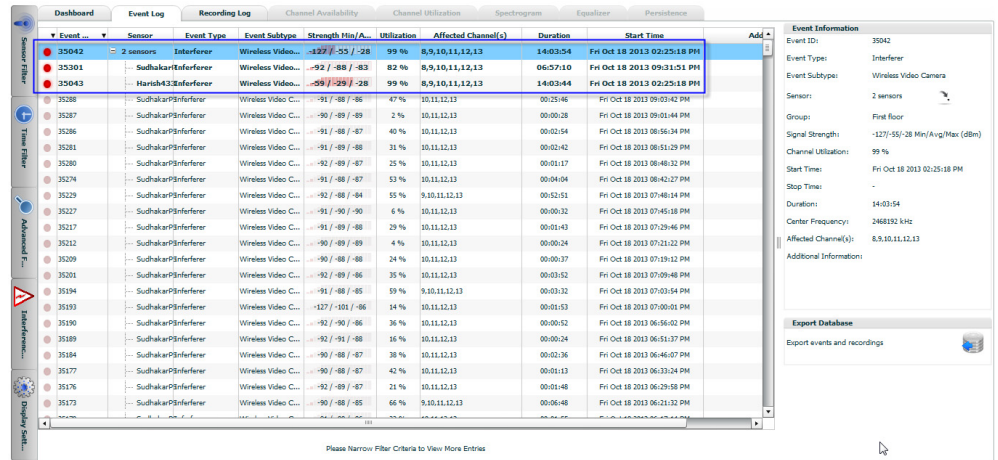
Interference Event Clustering

The *Spectrum Manager Event Log* screen displays the cluster of events. Multiple interference reports, correlated to the same interferer and interference event are assigned to the same

cluster ID. The interference event is reported as a single event, when multiple sensors report the same interference event.

Figure 145 on page 391 illustrates the *Interference Event Clustering* screen.

Figure 145: Interference Event Clustering



The *Spectrum Manager Event Log* screen provides various *Control Panel* tabs. For further information, refer to “*Control Panels*” on page 399.

Spectrum Manager - Recording Log

Spectrum Manager > Monitor > Dashboard > Recording Log

The *Spectrum Manager Recording Log* screen provides the log information of all Sensors. The following table depicts the *Recording Information* displayed on the *Recording Log* tab:

Field	Description
Recording ID	Displays the recording ID.
Recording Name	Displays the recording name.
Start Time	Displays the start time of recording.
Duration	Displays the duration of the recording

Field	Description
Sensor	<p>Displays the name of the selected <i>Sensor</i>. The following options are available for selection:</p> <ul style="list-style-type: none"> • <i>View live data from sensor</i>. <p>This option allows you to read the <i>live data from the Sensor</i>. The below mentioned tabs are enabled by the selection of the <i>View live data from sensor</i> option.</p> <ul style="list-style-type: none"> • Channel Availability • Channel Utilization • Spectrogram • Equalizer • Persistence <p>The above mentioned tabs reveal data of the selected <i>Sensor</i> in their respective tabs.</p>
Group	Displays the group name.
Recording State	Displays the recording state.
Recording Type	Displays the recording type.
Alert Type	Displays the alert type.
Alert Subtype	Displays the alert subtype.
Play recording	Select the <i>Play recording</i> option. This is used to playback the recording event.
Delete recording	Select the <i>Delete recording</i> option. This is used to delete the selected recording from the recording log page.



The above *Recording information* is also displayed on the right side of the Recording Log by selecting a Recording ID.

Scheduled and Configure Recordings

The recordings can be scheduled and configured by the following options:

1. *Schedule Recording*:

- Select the *Schedule Recording* icon.
- The *Schedule Recording* wizard is displayed. This wizard allows you to Start recording based on scheduled *Start* and *Stop* time.

- The *Schedule Recording* wizard allows you to provide the details for the following parameters:

Field	Description
Recording Name	Provide a recording name.
Start Time	Select the <i>Start Time</i> . The format followed is the <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format. Select the calendar icon to select the date. Select the time from the drop-down list.
Stop Time	Select the <i>Stop Time</i> . The format followed is the <i>mm/dd/yyyy</i> and <i>hh:mm:ss</i> format. Select the <i>calendar</i> icon to select the date. Select the time from the drop-down list.

- Select *Submit* to accept the changes.

2. *Alert-Triggered Recordings*:

- Select the *Alert-Triggered Recordings* icon.
- The *Alert-Triggered Recordings* wizard is displayed. This wizard allows you to start recording based on interference detection configuration or channel availability configuration.
- The *Alert-Triggered Recordings* wizard displays the *Interference Detection* tab and *Channel Availability* tab.
- *Interference Detection*:
The *Interference Detection* for the Recording Log is configured in a programmed manner. It automatically starts recording the FFT data when the specified interferer are detected based on the minimum RSSI and minimum duration. The maximum recording length is configured or the recording is allowed to continue until interferer is no longer active.
- *Channel Availability*:
The *Channel availability* for the Recording Log is configured in a programmed manner. It starts recording the FFT data when the channel quality drops below the configured minimum quality for a period exceeding a configured minimum duration. Alternatively, you can configure the system to start recording the FFT data when the channel utilization for WiFi, non-WiFi or total energy exceeds the configured maximum channel utilization for longer than the configured minimum duration.
- Perform selections on the *Interference Detection* tab and *Channel Availability* tab.
- Select *Submit* to accept the changes.

3. *Recording Database Maintenance*:

- Select the *Recording Database Maintenance* icon.
- The *Recording Database Maintenance* wizard is displayed. The *Recording Age Limit* and *Recording Purge Time* can be configured to delete the recording data. The default *Recording Age Limit* is configured to 3 Months, and the default *Recording Purge Time* is configured to 1:00 A.M.

Export Database

The *Export Database* option is used for debugging any fault event data, which can be exported to the Fortinet Customer Support for debugging analysis

- Select the *Export events and recordings* icon. The *Export Database* wizard is displayed.
- Provide a *Description* for the export of the recording. (optional step)
- The *Creating export database* file wizard is displayed.
- Select *Save*, to save the recording on the local hard disk.

The selected recording is exported to the local hard disk. One or more recordings can be selected and exported to the hard disk. A filter can be applied to the selected recordings and then exported to the hard disk. If no filters are applied, and no recordings are selected, the entire database is exported to the hard disk.

The *Spectrum Manager Recording Log* screen provides various *Control Panel* tabs. For further information, refer to “*Control Panels*” on page 399 topic.

Spectrum Manager - Channel Availability

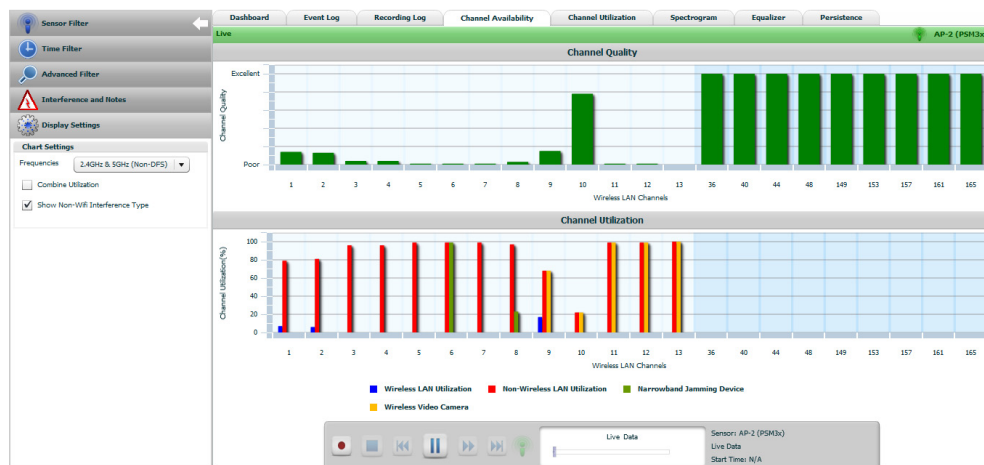
Navigation: Spectrum Manager > Monitor > Dashboard > Channel Availability

1. Select the *Channel Availability* tab.

The *Channel Availability* screen displays the *Channel Quality* and *Channel Utilization* graphs.

Figure 146 on page 394 illustrates the *Spectrum Manager Channel Availability* screen.

Figure 146: Spectrum Manager - Channel Availability



2. The *Channel Quality* and *Channel Utilization* graph, rendered in a flash application, displays a real time calculated channel quality for each of the Wi-Fi channels as well as the level of interference detected on each channel. The interference is differentiated between

802.11 interference and *Non-802.11* interference. The *Channel Utilization* graph also displays the *Channel Utilization* per Interference.

- Each of the interference is displayed as a percentage of the channel it is utilized.



The *Channel Utilization per Interference* type is displayed on the *Channel Utilization* graph, only if the *Show Non-Wifi Interference Type* option is checked in the *Display Settings*. This option is displayed only for the *Hardware Sensors* (See “*Hardware Sensors*” on page 412.)

- The *Channel Availability* screen provides various *Control Panel* tabs. For further information, refer to “*Control Panels*” on page 399.

Spectrum Manager - Channel Utilization

Spectrum Manager > Monitor > Dashboard > Channel Utilization

- Select the *Channel Utilization* tab.

Figure 147 on page 395 illustrates the *Spectrum Manager Channel Utilization* screen.

The *Channel Utilization* screen displays the *WLAN Channel Utilization* and *Non-WLAN Channel Utilization* graphs. This option is displayed only for the *Hardware Sensors* (See “*Hardware Sensors*” on page 412.)

Figure 147: *Spectrum Manager - Channel Utilization*



- The *WLAN Channel Utilization* and *Non-WLAN Channel Utilization* graphs, rendered in a flash application, displays a real time calculated channel utilization for each of the *WLAN* and *Non-WLAN* Channels.
- The *Channel Utilization* screen provides various *Control Panel* tabs. For further information, refer to “*Control Panels*” on page 399.

Spectrum Manager - Spectrogram

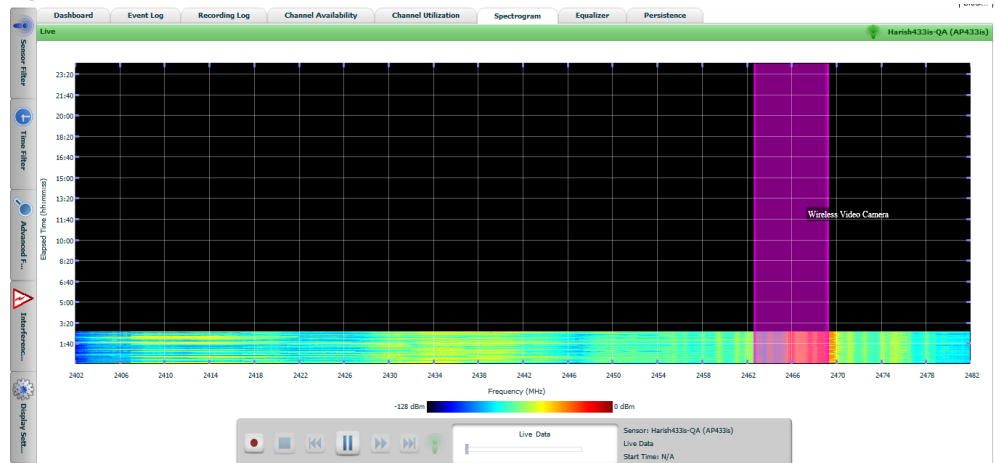
Navigation: *Spectrum > Monitor > Dashboard > Spectrogram*

1. Select the *Spectrogram* tab.

Figure 148 on page 396 illustrates the *Spectrum Manager Spectrogram* screen.

The *Spectrogram* screen provides the spectrum activity for the Interferer devices.

Figure 148: Spectrum Manager - Spectrogram



2. The scrolling *Spectrogram* displays the following details:
 - The frequency and amplitude of RF energy over time is displayed.
 - The *x-axis* displays the *Frequency (MHz)* or *Wi-Fi channel number*. The amplitude of the energy is plotted as *Instantaneous data* or the *maximum peak hold amplitude*. The amplitude is represented in blue color representing the weakest signal and red representing the strongest signal.
 - The *y-axis* displays the *Time*, with the most recent data at the bottom of the display and the plotted data scrolling upward.
3. The *Spectrogram* screen provides various *Control Panel* tabs. For further information, refer to *“Control Panels” on page 399*.

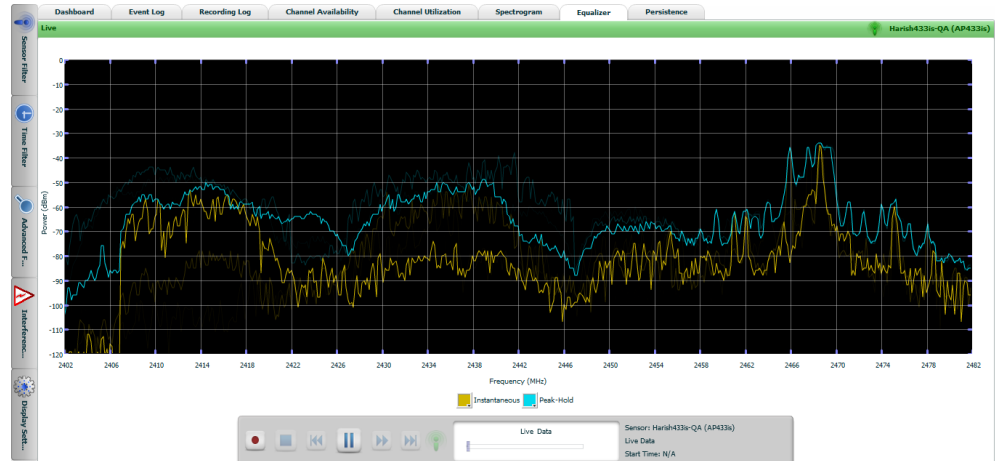
Spectrum Manager - Equalizer

Spectrum > Monitor > Dashboard > Equalizer

1. Select the *Equalizer* tab.

Figure 149 on page 397 illustrates the *Spectrum Manager Equalizer* screen.

Figure 149: Spectrum Manager - Equalizer



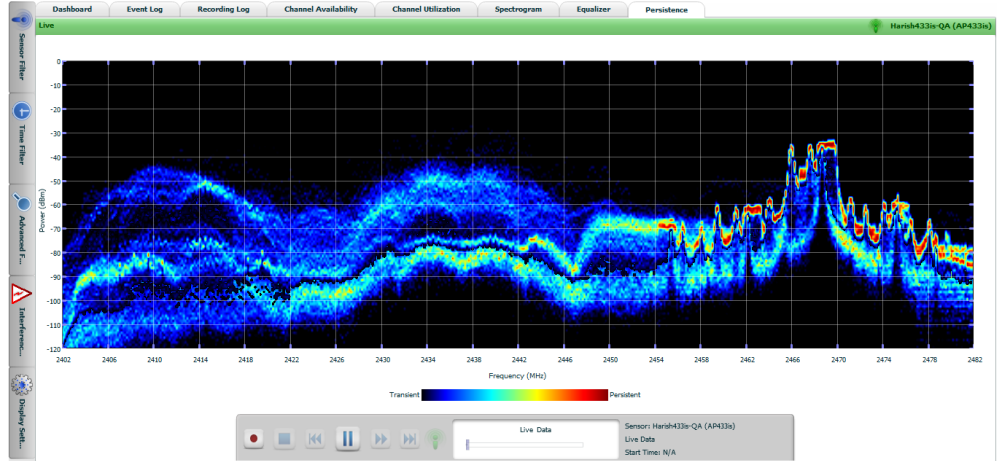
2. The *Equalizer* screen provides a flash application that starts *Sensor* to the browser. The *Equalizer* is a plot of the *amplitude* versus the *frequency* of RF (RF Energy or Signal) scanned by the “*Sensors*” on page 412.
3. The *Spectrum Equalizer* plots the *amplitude* vs. *frequency* for the detected RF energy. The frequency along the x-axis can be displayed as either frequency (MHz) or Wi-Fi channels. Both the instantaneous amplitude (the last data point collected over the scan period) and the maximum peak hold amplitude (the highest data point collected over the scan period) are dynamically plotted. The instantaneous data is plotted in yellow, while the peak hold data is plotted in blue. The colors are user configurable.
4. The *Equalizer* screen provides various *Control Panel* tabs. For further information, refer to “*Control Panels*” on page 399.

Spectrum Manager - Persistence

Spectrum > Monitor > Dashboard > Persistence

1. Select the *Persistence* tab.
Figure 150 on page 398 illustrates the *Spectrum Manager Persistence* screen.

Figure 150: Spectrum Manager - Persistence



2. The *Persistence* screen provides a flash application. The Persistence provides the spectrum activity for the Interferer devices to view the channel Persistence link to display the interference events.
3. The *Persistence* display plots the *amplitude vs. frequency* for the detected RF energy. Both the instantaneous amplitude (the last data point collected over the scan period) and the maximum peak hold amplitude (the highest data point collected over the scan period) are dynamically plotted. The color of a pixel on the display represents the number of times the energy was detected at that specific frequency and amplitude, with blue representing the least frequent and red representing the most frequent.
4. The *Persistence* screen provides various *Control Panel* tabs. For further information, refer to [“Control Panels” on page 399](#).

Control Panels

The *Control Panels* are displayed towards the left of the *Dashboard* screen.

The following table depicts the various *Control Panel* tabs available on the *Monitor Console* screen:

- [“Sensors Filter” on page 399](#)
- [“Sensors Hierarchy” on page 399](#)
- [“Advanced Filter” on page 402](#)
- [“Interference and Notes” on page 403](#)
- [“Display Settings” on page 404](#)

Sensors Filter






The *Sensors Filter* enables to filter the information to be displayed on the screen by selecting a sensor under sensor hierarchy. Perform the following steps to configure the Sensors filter:

- Select the *Sensors Filter* tab. A list of sensors deployed is displayed.
- Select a sensor in *Sensor hierarchy* and click on *Filter selected Group/sensor*. The following changes also occur:
 - The selected sensor is displayed on *Trend Graph*, *Interferer Type* and *Affected Channels* sections of the *Dashboard* screen.
 - The *Event Log* details are updated with selected sensor in *Event Log* screen.
 - The *Recording Log* details are updated with selected sensor on *Recording Log* screen.
- The *Sensors Filter* tab displays the following two sections:
 - [“Sensors Hierarchy” on page 399](#)
 - [“Group Information” on page 400](#)

Sensors Hierarchy

The *Sensors Hierarchy* section displays the sensors hierarchically belonging to an *Enterprise*, or a *Building* within an *Enterprise*, or a *Floor*, and the APs ([“Software Sensors” on page 412](#) and [“Hardware Sensors” on page 412](#)) listed within the *Floor*.

- The following table displays the icons provided for a hierarchy of *Enterprise*, *Campus*, *Building*, *Floor* and *AP*.

Term	Description
Enterprise 	Enterprise is the top most level where the <i>Campus</i> , <i>Building</i> , <i>Floor</i> and <i>AP</i> can be added.
Campus 	<i>Campus</i> icon adds a campus to the top level, <i>Enterprise</i> , which is the default.
Building 	<i>Building</i> icon adds a new Building to the Campus level.
Floor 	<i>Floor</i> icon adds a new Floor to the Building level.
AP 	<i>AP</i> icon adds a new AP to the Floor level.

Group Information

The *Group Information* section provides the details of the selected *Enterprise*, *Campus*, *Building*, *Floor* and *AP*.

- The following details for the selected *Enterprise*, *Campus*, *Building*, *Floor* and *AP* are displayed:
 - Name - Displays the name of the sensor.
 - Description - Displays the MAC address of the sensor.
 - IP Address - Displays the IP address of the sensor
 - Status - Displays the connection status of the sensor.
- Select an *Enterprise*, *Campus*, *Building*, *Floor* or *AP* from the above *Sensors Hierarchy* section.
- Select the *Filter Selected Group/Sensor* option.
- The graph for the selected sensor is displayed on *Trend Graph*, *Interferer Type* and *Affected Channels* sections of the *Dashboard* screen.

The *Sensors Filter* tab is enabled only in the below mentioned tabs:

- Dashboard
- Event Log
- Recording Log

Time Filter

The *Time Filter* enables to configure the screen to display information over a period of time. This can be performed by configuring the *Start Time* and *Stop Time* parameters on the page.

Perform the below actions to configure the *Time Filter*:

- Select the *Time Filter* tab.
- The *Time Filter* tab displays the following two sections:
 - “*Start Time*” on page 401
 - “*Stop Time*” on page 401

Start Time

- Select the option *Earliest Time Possible*. The system fetches the data available for the earliest possible time.
- Uncheck the *Earliest Time Possible* option to select the *Start Time*.
- From the *Time* option, select the time from the drop-down list. The format followed is *hh:mm:ss* format.
- From the *Date* option, select the calendar icon to select the *Month*, *Date* and *Year*. The format followed is the *mm/dd/yyyy*.

Stop Time

- Select the option *Use Current Time*. The system applies the current time.
- Uncheck the *Use Current Time* option to select the *Stop Time*.
- From the *Time* option, select the time from the drop-down list. The format followed is *hh:mm:ss* format.
- From the *Date* option, select the calendar icon to select the *Month*, *Date* and *Year*. The format followed is the *mm/dd/yyyy*.
- Select *Apply Time Filter* option.
- The *Time Filter* is applied to the *Trend Graph*, *Interferer Type* and *Affected Channels* sections of the *Dashboard* screen.



The Controller time and *FortiWLM* time must be in Sync.

The *Time Filter* tab is applied and enabled to the below mentioned tabs:

- Dashboard
- Event Log

- Recording Log

Advanced Filter

The *Advanced Filter* option enables to configure the information to be displayed on the screen by choosing the following available filters:

- Channel Filter
 - This filter enables you to filter the information based on the available channels.
 - Select the desired channel from the *Channel* list.
 - Select *Apply Filter*. The *Channel Filter* is applied to the *Dashboard* screen and the *Event Log* screen.
- RSSI Filter
 - This filter depicts the signal strength of the Interferer device.
 - Select the desired *RSSI* value from the *RSSI Filter* list. The values displayed are in dBm.
 - Select *Apply Filter*. The *RSSI Filter* is applied to the *Dashboard* screen and the *Event Log* screen.
- Interferer Type
 - This filter depicts the Interferer Type.
 - A list of Interferer Type options is available for selection.
 - Select the desired *Interferer Type*.
 - Select *Apply Filter*. The *Interferer Type* filter is applied to the *Dashboard* screen.



The above mentioned Interferer type *Advanced Filter* options is enabled only on the *Dashboard* screen.

- Event Log Type
 - This filter depicts the *Event Log Type* (*Alert Event* or *Interferer Log Event*).
 - A list of *Interferer Log Events* and *Alert Event* options is available for selection in the *Event log* subtype.
 - Select the desired Event Log Type and select desired Event Subtype.
 - Select *Apply Filter*. The *Event Log Type/Subtype* filter is applied to the *Event Log* screen.



The above mentioned *Advanced Filter* option is enabled only on the *Event Log* screen.

- Recording Type
 - This filter depicts the Recording Type.
 - A list of Recording Type options is available for selection. The types are as follows:
 - Alert-Triggered Recording
 - Manual Recording
 - Scheduled Recording
 - Select the desired Recording Type.
 - The selected *Recording Type* filter is applied to **Recording Log** screen.
- Recording State
 - This filter depicts the Recording State.
 - A list of *Recording State* options is available for selection. The types are as follows:
 - Pending
 - Active
 - Completed
 - Failed
 - Select the desired Recording state.

The selected Recording State filter is applied to Recording Log screen



The above mentioned *Advanced Filter* options is enabled on the *Recording Log* screen.



The *Advanced Filter* tab is enabled only in the below mentioned tabs:

Dashboard

Event Log

Recording Log

Interference and Notes

The *Interference and Notes* section displays the following:

Start Time: This is the *Start Time* of the interference and interference type.

- *Add Note*: The *Add Note* icon enables to add a note.



The *Notes* section is enabled only on the completion of manual recording. The *Notes* section displays the following:

Delete Note - The *Delete Note* icon enables to delete a note.

Timestamps - The *Timestamp* is used to adjust the *Current Recording* playback time to the Time stamp of the note.

The *Interference and Notes* option is displayed on the following tabs:

- Channel Availability
- Channel Utilization
- Spectrogram
- Equalizer
- Persistence

Display Settings

The *Display Settings* option enables to configure the information to be displayed on the following screens:



The *Display Settings* tab is enabled only in the below mentioned tabs.

- Event Log
 - Recording Log
 - Channel Availability
 - Channel Utilization
 - Spectrogram
 - Equalizer
 - Persistence
-

Event Log - Display Settings

Perform the following actions to select the columns to be displayed on the *Event Log* screen:

- Select the *Event Log* tab. The *Event Log* screen is displayed.
- Select the *Display Settings* tab.
- Select the desired columns to be displayed.

- The selected columns are displayed on the *Event Log* screen.



Select the *Apply Default Column Setting* option to display the default columns.

Recording Log - Display Settings

Perform the following actions to select the columns to be displayed on the *Recording Log* screen:

- Select the *Recording Log* tab. The *Recording Log* screen is displayed.
- Select the *Display Settings* tab.
- Select the desired columns to be displayed.
- The selected columns are displayed on the *Recording Log* screen.



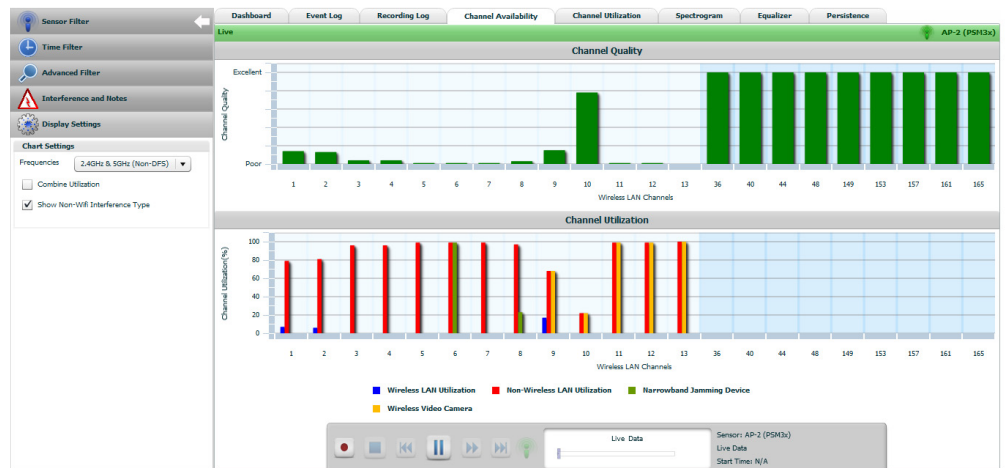
Select the ***Apply Default Column Setting*** option to display the default columns.

Channel Availability - Display Settings

Perform the following actions to modify the graphical display of the *Channel Availability* screen:

- Select the *Channel Availability* tab. The *Channel Availability* screen is displayed.
- Select the *Display Settings* tab. ([Figure 151 on page 406](#) illustrates the *Channel Availability* screen of the *Display Settings*.)
- The *Chart Settings* option is displayed.

Figure 151: Display Settings - Channel Availability



- Select the *Frequencies* from the drop-down list to view the *Channel Quality* and *Channel Utilization* on the respective channels. The *Display Frequency* can be set to scan the 2.4 GHz frequency band, the 5 GHz frequency band or *both*.
- Select the *Combine Utilization* option. This enables the *Channel Utilization* graph (which is in channel quality) to combine the *Non-Wireless LAN Interference* and *Wireless LAN Interference*.

Channel Utilization - Display Settings

Perform the following actions to modify the graphical display of the *Channel Availability* screen:

- Select the *Channel Utilization* tab. The *Channel Utilization* screen is displayed.
- Select the *Display Settings* tab.
- The following sections are displayed: ([Figure 152 on page 407](#) illustrates the *Channel Utilization* screen of the *Display Settings*.)
 - “[Timescale settings](#)” [on page 406](#)
 - “[Channel selection settings](#)” [on page 406](#)

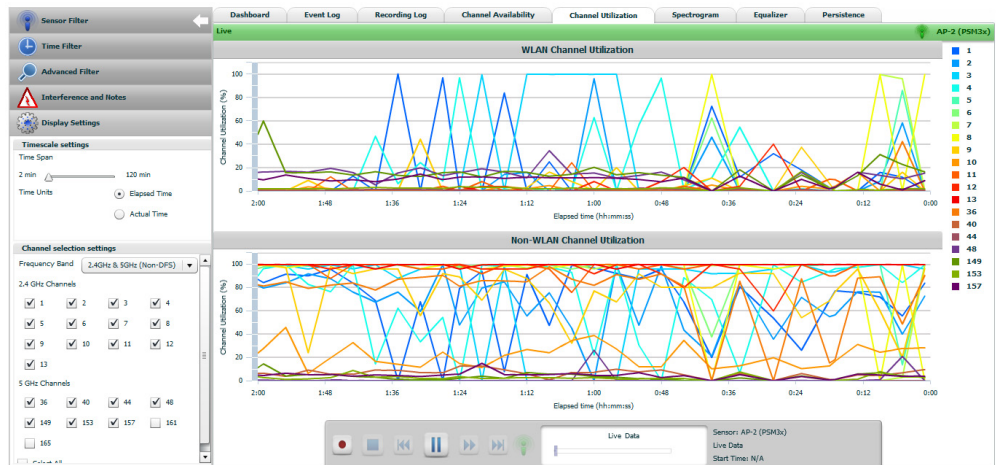
Timescale settings

- Select the *Time Span*. The valid range is between 2 min - 120 min.
- Select the *Time Units*. The Time Units allows you to select the *Elapsed Time* or *Actual Time*.

Channel selection settings

Select the *Frequency Band* from the drop-down list.

The *Select All* option enables to display all the *WLAN Channel Utilization*.
Figure 152: Display Settings - Channel Utilization



Spectrogram - Display Settings

The Spectrogram - Display Settings provides the following options:

1. **Data**
 - Select the *Data* option. The *Data* option allows you to select the *Instantaneous* data or *Peak* data.
2. **Time Span**
 - Select the *Time Span*. The *Time Span* ranges between *Long* - *Short*.
3. **Axis**
 - Select the *Axis* type. The *Axis* is configured based on *Frequency* and *Wi-Fi Channels*.
Frequency: This option displays the graph based on the frequency.
Wi-Fi Channels: This option displays the graph based on the *Wi-Fi Channels*. Select the *Wi-Fi Channels* option, the following parameters are displayed:
 - *Highlight Channel*: Check the *Highlight Channel* option, to highlight a channel when the channel in the x-axis is being mouse-over.
 - *Wi-Fi Channel Width*: Select the *Wi-Fi Channel Width* from the drop-down list. This sets the channel width for the spectrogram to display. Select any one option from the drop-down list. The options are *20Mhz*, *20Mhz+Upper 20 Mhz* and *20Mhz+Lower 20 Mhz*.



The *Wi-Fi Channel Width* option is enabled only when the *Axis* selected is *Wi-Fi Channels*.

4. Band

- Select one option from the *Band* list.
- The Spectrogram for the respective bands can be set by selecting one of the options from the drop-down list.
- The options is *2.4GHz*, *5GHz (Lower)* and *5GHz (Upper)*.



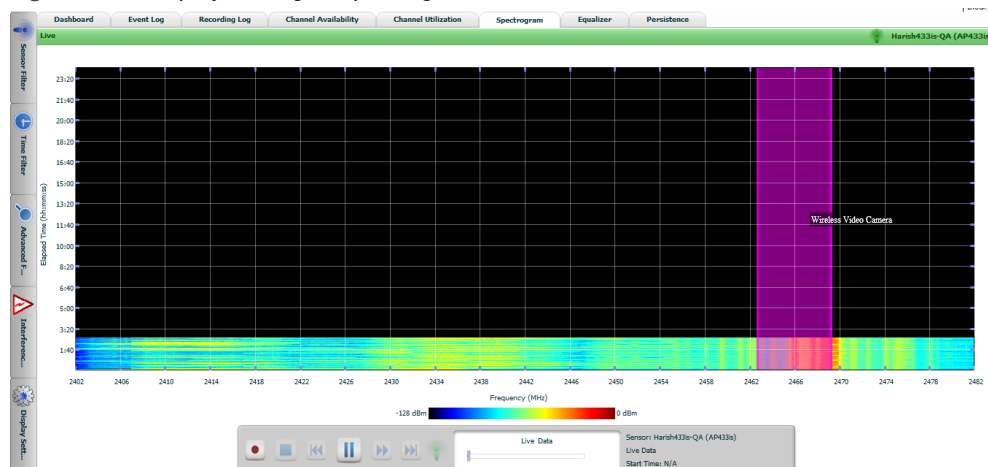
The transient and spectrogram measure is displayed accordingly, to the color fading.

5. Overlay Interference - This option highlights the spectrum activity for a particular interferer.

For Example: In the scenario where more interference events are noticed and if the particular interferer is to be viewed, then the overlay for that interferer device can be checked.

([Figure 153 on page 408](#) illustrates the *Spectrogram* screen of the *Display Settings*.)

Figure 153: Display Settings - Spectrogram



Markers

1. Select the *Spectrogram* tab. The *Spectrogram* screen is displayed.
2. Select the *Display Settings* tab.
3. Select the *Markers* section.
4. The markers can be used to visually mark a Frequency on the *Spectrogram* plot.
5. Check a marker in the Markers section, the marker appears on the *Spectrogram* graph.
6. Select the marker on the display to move it to the desired frequency to visually mark off.

Equalizer - Display Settings

The *Equalizer - Display Settings* provides the following options:

1. Persistence

- Select the *Persistence* range.
- Setting *Persistence*, allows us to study the timed trends in the graph. Increasing the persistence of the display increases the amount of time that samples are retained and displayed allowing us to study variations over time. This can be set in the bar on the display settings from *Zero* to *Infinity*.

Figure 154 on page 410 illustrates the *Equalizer* screen of the *Display Settings*.

2. Axis

- Select the *Axis* type. The *Axis* is configured based on *Frequency* and *Wi-Fi Channels*.
 - *Frequency*: This option displays the graph based on the frequency.
 - *Wi-Fi Channels*: This option displays the graph based on the *Wi-Fi Channels*. Select the *Wi-Fi Channels* option, the following parameters are displayed:
 - *Highlight Channel*: Check the *Highlight Channel* option, to highlight a channel when the channel in the x-axis is being mouse-over.
 - *Wi-Fi Channel Width*: Select the *Wi-Fi Channel Width* from the drop-down list. This sets the channel width for the spectrogram to display. Select any one option from the drop-down list. The options are *20Mhz*, *20Mhz+Upper 20 Mhz* and *20Mhz+Lower 20 Mhz*.



The *Wi-Fi Channel Width* option is enabled only when the *Axis* selected is *Wi-Fi Channels*.

1. Band

- Select one option from the *Band* list.
- The Equalizer for the respective bands can be set by selecting one of the options from the drop-down list.
- The options is *2.4GHz*, *5GHz (Lower)* and *5GHz (Upper)*.

Figure 154: *Display Settings - Equalizer*



Markers

1. Select the *Equalizer* tab. The *Equalizer* screen is displayed.
2. Select the *Display Settings* tab.
3. Select the *Markers* section.
4. The markers can be used to visually mark a Frequency on the *Equalizer* plot.
5. Check a marker in the Markers section, the marker appears on the *Equalizer* graph.
6. Select the marker on the display to move it to the desired frequency to visually mark off.

Persistence - Display Settings

The Persistence Settings provides the following options:

1. Persistence
 - Select the Persistence range.
 - Setting Persistence, allows us to study the timed trends in the graph. Increasing the Persistence of the display increases the amount of time that samples are retained and displayed allowing us to study variations over time. This can be set in the bar on the display settings from *Zero* to *Infinity*.

Figure 155 on page 411 illustrates the *Persistence* screen of the *Display Settings*.
2. Axis
 - Select the *Axis* type.
 - The *Axis* is configured based on *Frequency* and *Wi-Fi Channels*.
 - *Frequency*: This option displays the graph based on the frequency.
 - *Wi-Fi Channels*: This option displays the graph based on the *Wi-Fi Channels*. Select the *Wi-Fi Channels* option, the following parameters are displayed:

Highlight Channel: Check the *Highlight Channel* option, to highlight a channel when the channel in the x-axis is being mouse-over.

Wi-Fi Channel Width: Select the *Wi-Fi Channel Width* from the drop-down list. This sets the channel width for the spectrogram to display. Select any one option from the drop-down list. The options are *20Mhz*, *20Mhz+Upper 20 Mhz* and *20Mhz+Lower 20 Mhz*.

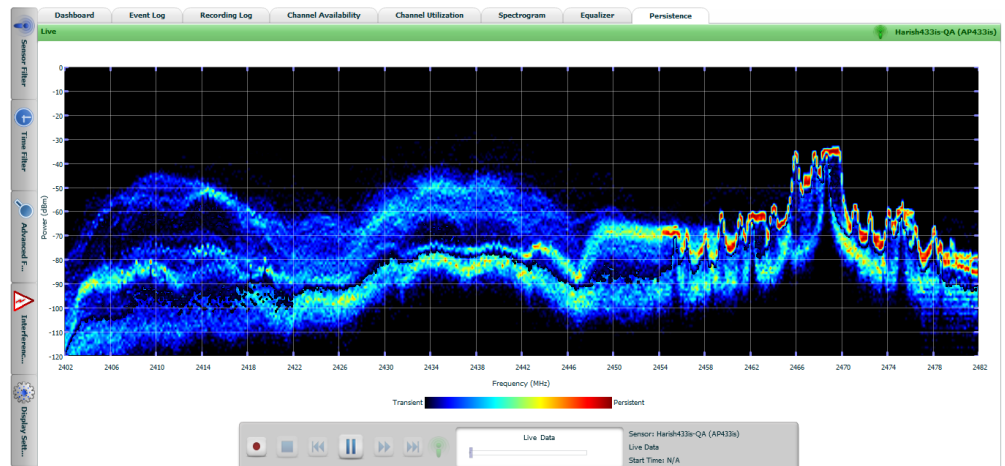


The *Wi-Fi Channel Width* option is enabled only when the *Axis* selected is *Wi-Fi Channels*.

1. *Band:*

- Select one option from the *Band* list.
- The Equalizer for the respective bands can be set by selecting one of the options from the drop-down list.
- The options is *2.4GHz*, *5GHz (Lower)* and *5GHz (Upper)*.

Figure 155: Display Settings - Persistence



Markers

1. Select the *Persistence* tab. The *Persistence* screen is displayed.
Figure 155 on page 411 illustrates the *Persistence* screen of the *Display Settings*.
2. Select the *Display Settings* tab.
3. Select the *Markers* section. The markers can be used to visually mark a Frequency on the *Persistence* plot.
4. Check a marker in the Markers section, the marker appears on the *Persistence* graph.
5. Select the marker on the display to move it to the desired frequency to visually mark off.

Sensors

The *Sensors* are classified as follows:

Software Sensors

The software-based sensor is a normal AP with one Radio in ScanSpectrum Mode. Here, the AP mode can be modified from Service/Normal Mode to ScanSpectrum Mode.

Note:

- The modification of AP mode from **Service/Normal Mode** to **ScanSpectrum Mode** can be performed only via the FortiWLC GUI or by pushing the AP template with Radio profile configured with the **ScanSpectrum Mode** from FortiWLM.
- You can configure both radios of FAP-U421EV, FAP-U423EV, FAP-U321EV, FAP-U323EV sensors in **ScanSpectrum Mode**, which will make the radios to scan both the Radio spectrum for interference. For all the other Sensors, only single radio can be configured in **ScanSpectrum Mode** at a time.
- No client service will be provided once Radios are configured in the **ScanSpectrum Mode**.

The *Software Sensors* include the following *Access Points*:

- AP1014i
- AP1010i
- AP1010e
- AP1020i
- AP1020e
- AP332i
- AP332e
- AP832i
- AP832e
- FAP-U421EV
- FAP-U423EV
- FAP-U321EV
- FAP-U323EV

Hardware Sensors

The Hardware-based sensors are completely dedicated to monitor the airwaves of the time. By having a dedicated subsystem, the sensor can classify and report on the type and source

of interference almost instantly and without taking CPU resources away from the wireless radio. The *Hardware Sensors* include the following *Access Points*:

- PSM3x
- AP433is

RF Interferer Classification

Wi-Fi networks operate in the unlicensed 2.4 and 5 GHz frequency bands, where they share a medium with a variety of other devices. With the exception of Bluetooth devices, none of the other devices have any mechanisms to co-exist with Wi-Fi networks. As a result, when an interfering device is emitting energy in the WLAN channel the WLAN Access Point is used for communication, the throughput of the AP can be significantly affected.

Spectrum detects all non-802.11 interference devices, especially the devices mentioned in the below list:

- Microwave ovens (conventional)
- Microwave ovens (inverter)
- Motorola Canopy Wireless
- Non-Wifi Wireless Bridges
- Wireless video cameras (digital and analog)
- Analog cordless phones (2.4GHz and 5GHz)
- FHSS cordless phones (2.4GHz and 5GHz)
- DSSS cordless phones (2.4GHz and 5GHz)
- Bluetooth devices
- Wireless baby monitors
- Game Controllers
- RF Jammers (both narrowband and wideband)
- Wireless mice
- Zigbee devices
- Motion Detectors (S-band, radar-based)

In addition to the above mentioned devices, the RF Jamming devices also exist. The RF Jamming devices can be used to intentionally interfere with wireless communications. Although, these devices are considered to be illegal in the US and elsewhere, they provide performance and security issues to WLANs.

Wireless LANs based on the IEEE 802.11 standards, function in the unlicensed 2.4 and 5 GHz frequency bands. Other devices emitting radio-frequency energy in these bands can interfere

with WLAN transmissions. The *“Radio frequency characteristics for the interferer devices listed below” on page 415* lists some common RF interferer and their RF characteristics.

Radio frequency characteristics for the interferer devices

The Radio frequency characteristics for the interferer devices are listed below:

From the deployment perspective, the Spectrum coverage not only depends upon its sensor (receiver sensitivity), but also depends upon the interference devices transmit power (or signal strength). We cannot place the sensors far away and expect the very low signal strength interference device packets to reach the sensor.

Theoretically, lower the signal strength of the interference devices more sensors must be packed to catch those devices.

The *“Sensors” on page 412* (*“Software Sensors” on page 412* and *“Hardware Sensors” on page 412*) must be installed at least six feet away from a servicing AP. Having it closer affects the accuracy of interference classification.



The servicing APs must not be installed very close to PSM3x, as the false events (Analog Cordless Phones, etc.,) may be detected by PSM3x sensor due to the EMI (Electromagnetic Interference) emitted near by APs.

For Example:

Bluetooth has 2.2 dBm transmit power, for which the sensors must be placed closer in the given site, for it to be captured. So, the signal strength of interference devices is inversely proportional to the sensors coverage area.

Also the sensor coverage area is proportional to the receiver sensitivity. More the receiver sensitivity (which can be obtained with higher gain antennas) the sensors can be more sparsely distributed compared to the above example.

The conclusion is, the coverage area of the sensor depends upon the lowest signal strength of the interference device to be detected and depends upon the receiver sensitivity of the sensor. More the signal strength of the interference device and more the receiver sensitivity, the sensors will have more coverage and vice versa. Assuming the above considerable factors the predictable coverage can be identified with the following table, which has a specified interfer-

ence transmit power. So it's the administrator or the user environment the deployment for the sensors can be predicted.

TABLE 3: *Radio frequency characteristics for the interferer devices listed below*

Interferer Device	Frequency Range	Transmit Power	Modulation	# Communication Channels Supported	Width	Features
Bluetooth	2402-2480 MHz	2.2 dBm	GFSK, FHSS	79	1 MHz	Pulsed, low-power
Analog Cordless Phone	2403-2480 MHz	NA	Narrow Band FM	40	~300 kHz	Narrow Band FM
DSSS Digital Cordless Phone	2407.5-2472 MHz	20 dBm	DSSS	40	1.5 MHz	High-power, duty Factor
FHSS Digital Cordless Phone	2408.5-2472 MHz	21 dBm	FHSS	90	892 kHz	Pulsed, high-power
Conventional Microwave Oven	2.4 GHz	800W	N/A	N/A	N/A	Pulsed, broadband
Inverter Microwave	2.4 GHz	1300W	N/A	N/A	N/A	Pulsed, broadband
Wireless Video Camera	2414 – 2468 MHz	10 dBm	Frequency Modulation (FM)	4	N/A	Broad-band, high-power
Digital Video Monitor	2402 – 2483 MHz	20 dBm	FHSS	27	2MHz	High-power, frequency hopping
Game Controller	2402 – 2482 MHz	N/A	FHSS	40	500kHz	Pulsed, low-power, Frequency hopping

17 Sensors

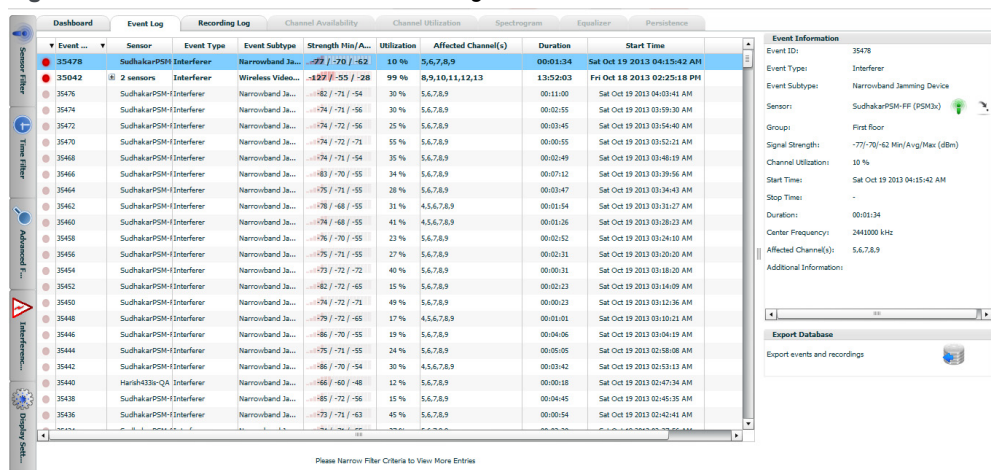
RF Interferer Detection

With the WLANs supporting critical applications such as voice and video communications, monitoring and management of RF interference becomes a security imperative. Interference can be from an intentional, malicious interferer such as an RF jammer or from an unintentional source such as a cordless phone in a nearby location. In either case, the ability of the WLAN to support the real-time communication required by these applications can be severely compromised by the RF interference. WLANs must be able to continuously detect the interferer in the RF environment for these security issues and trigger alerts to network administrators.

The *Sensors* which are listed in the *Event Log* page provides the interference event information.

Figure 156 on page 417 illustrates the sensors listed on the Event Log screen.

Figure 156: Sensors listed on the Event Log screen



Each interferer device signal is treated as an interference event and is detected by the following parameters:

- Event Subtype (Type of interferer)

- Signal Strength (Current/ Average / Maximum) dBm
- Affected Channel(s) (Impact will be on the channels listed)
- Center frequency
- Duration (how long the inference event was seen)
- Start Time (At what time the interference event started)
- Stop Time (At what time the interference event stopped)

The active Interference event is highlighted in bold font and a red dot.

The event which is not alive at the moment will be grayed out as shown in the

The RF Interferer classification is detected by the following parameters

- Channel
- Signal Strength
- Interferer.

Interferer can be detected,

- By opting to filter, for only on that channel.
- Interferer fading into the 2.4GHz and the 5GHz spectrum by varying its signal strength which is detected by opting to filter the signal strength ranging from ≥ -10 dBm to ≥ -110 dBm
- By Specific interferer devices.
Interferer on all channels, in the range of signal strength and also on all types of Interferer devices can also be filtered by opting "All".

Historical Spectrum dashboard Analysis

Spectrum Manager provides historical spectrum data for analysis. The impact on the interferer devices can be determined with the data available from the past with the tentative date and time. Interference events caused by the interferer devices are stored in the *Spectrum Manager* database for future analysis. A history of interference events for one year is maintained.

Event logs

The triggered events from the particular sensor are consolidated, captured and displayed in the Event Log screen as displayed in [Figure 144 on page 389](#).

Time-based Analysis

The *Spectrum* events are the time-based triggered events, for which the "Start and Stop time" is not provided. It must display the dashboard for the current interference activity. Ensure the

“Earliest Time possible in Start time and Use current time in Stop time” check box is checked, to view the dashboard for real time display.

A

Appendix A - Virtual Edition

FortiWLM introduces a new feature the *Virtual Edition* which is a *Virtual Edition* of the *Application Suite* (*Service Assurance Manager* and *Spectrum Manager*).

The following virtual software platforms are supported:

- VMware
 - ESX v4.0 and v4.1
 - ESXi v4.0, v4.1, v5.0 and v5.1

The setup of *FortiWLM* is performed on the VMware platform through the *vSphere Client*. The *VMware vSphere Client* is an interface that allows virtual machine management and access to the *ESXi* server from a *Windows PC*.

Fortinet E(z)RF VE platform is equivalent to *SA2000* with respect to scalability and configuration and called *SA2000-VE*.

The following table provides the resource requirement details of the *FortiWLM* on the *VMware* platform.

Feature	VMware
Disk Storage	500GB
RAM	8 GB
Number of CPUs	4
Ethernet Adaptor Type	E1000

To set up the *FortiWLM* on the *VMware platform*, follow the below mentioned steps:

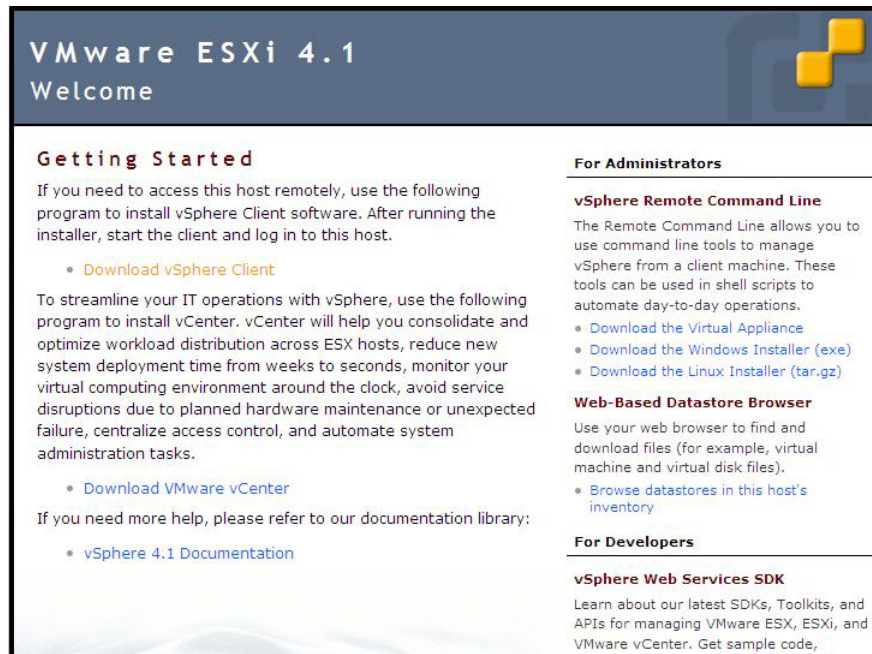
Install and Configure VMware

Configure VMware and assign an IP address.

Download vSphere Client

Download the **vSphere Client** from the IP address. See [Figure 157 on page 422](#).

Figure 157: *Download vSphere Client*



The “*Install and Configure VMware*” and “*Download vSphere Client*” sections are optional. It is applicable only for initial VMware setup.

Login to the vSphere Client

After you download the **vSphere Client**, the below mentioned steps are implied in installation:

1. Login to the **vSphere Client** using IP Address.
2. Provide the **User Name** and **Password**.

Create Virtual FortiWLM using vSphere client

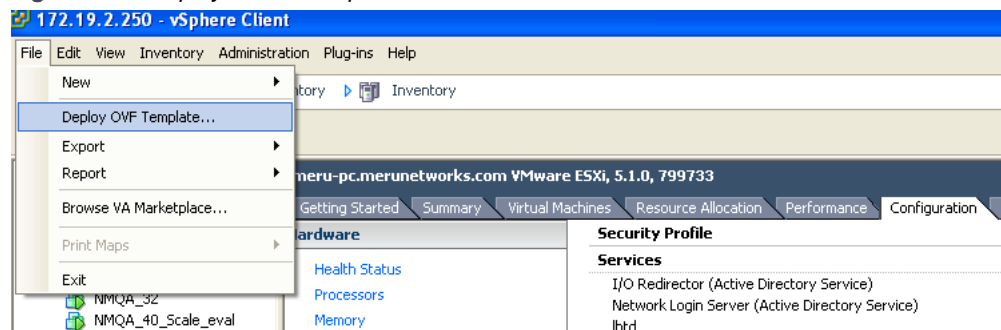
The Virtual FortiWLM can be created using,

- .ova file (See “[Create Virtual FortiWLM using .OVA file](#)” on page 423)
- .vmx and .vmdk file (See “[Create Virtual FortiWLM using .vmx and .vmdk file](#)” on page 427)

Create Virtual FortiWLM using .OVA file

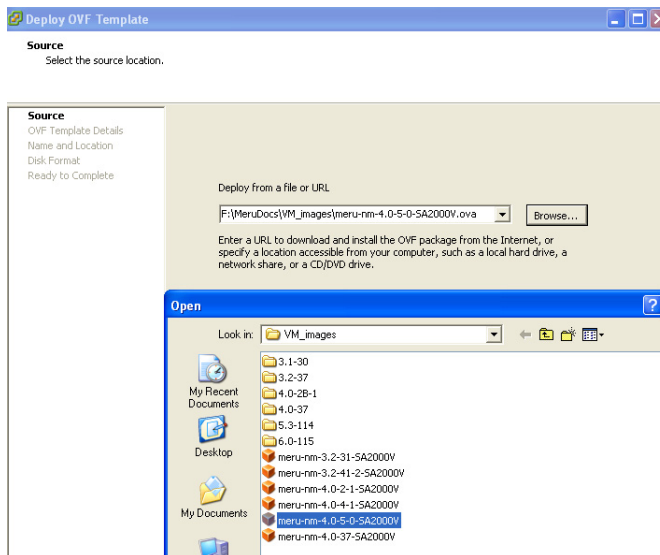
1. Copy .ova format image file to a location on your local hard drive.
For Example: FortiWLC-4.0-5-0-SA2000V.
2. Launch Vsphere client and navigate to *File > Deploy OVF template*.

Figure 158: Deploy OVF Template



3. Browse the .ova format image source file as displayed in [Figure 159 on page 423](#).

Figure 159: Source - ova file format



4. Select the ova file and select *Next*.
5. In the *OVF Template Details*, verify the details. Ensure the size on the disk is more than 500GB [thick provisioned] and click *Next*. See [Figure 160 on page 424](#).

Figure 160: OVF Template Details

The screenshot shows a window titled "Deploy OVF Template" with a blue header bar. Below the header, the main content area is titled "OVF Template Details" with the instruction "Verify OVF template details." On the left, there is a sidebar with a list of steps: "Source", "OVF Template Details" (which is highlighted), "Name and Location", "Disk Format", "Network Mapping", and "Ready to Complete". The main area displays the following details for the template:

Product:	meru-sa2000v
Version:	
Vendor:	
Publisher:	No certificate present
Download size:	301.3 MB
Size on disk:	601.4 MB (thin provisioned) 501.9 GB (thick provisioned)
Description:	

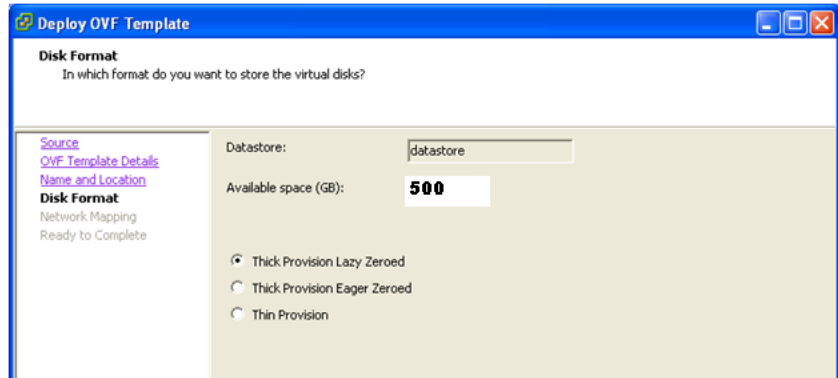
6. In the *Name and Location*, specify the name and location for the deployed template. The name can contain up to 80 characters and must be unique within the inventory folder. Click *Next*. See [Figure 161 on page 424](#).

Figure 161: Name and Location

The screenshot shows the same "Deploy OVF Template" window, but now the "Name and Location" step is highlighted in the sidebar. The main content area is titled "Name and Location" with the instruction "Specify a name and location for the deployed template". It features a text input field labeled "Name:" with the value "meru-sa2000v" entered. Below the input field, a message states: "The name can contain up to 80 characters and it must be unique within the inventory folder."

7. In the *Disk Format*, choose the format in which you want to store the virtual disks. Choose the default option, *Thick Provisioned Lazy Zeroed*. See [Figure 162 on page 425](#).

Figure 162: *Disk Format*



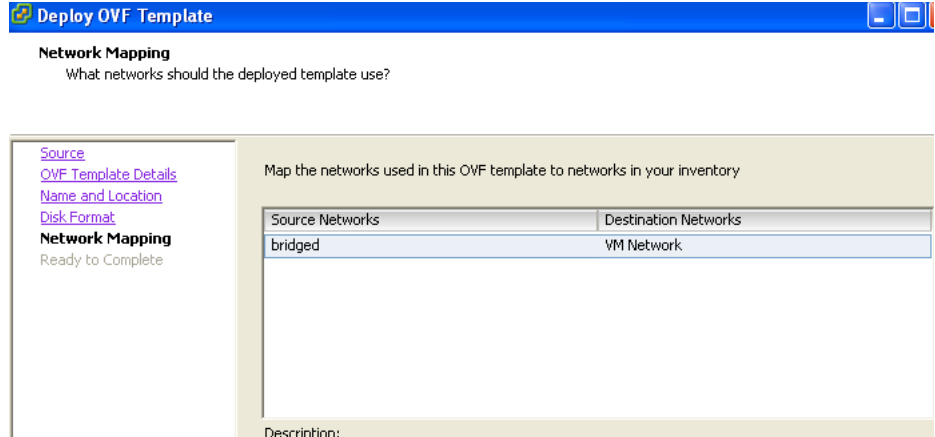
Following are the three options in which you want to store the virtual disks.

- **Thick Provision Lazy Zeroed:** The virtual disk allocates all of its provisioned space and is immediately accessible to the virtual machine. A lazy zeroed disk is not zeroed upfront which makes the provisioning very fast. However, because each block is zeroed out before it is written to for the first time there is added latency on first write.
- **Thick Provision Eager Zeroed:** The virtual disk is allocated all of its provisioned space and the entire VMDK file is zeroed out before allowing the virtual machine access. This means that the VMDK file will take longer to become accessible to the virtual machine, but will not incur the additional latency of zeroing on first write. For this reason the recommendation when deploying an I/O intensive application on VMFS is to use this provisioning method.
- **Thin Provisioning:** This method provides quick access to the virtual disk and increases storage utilization by allocating disk space on demand.

Select “*Thick Provisioning Lazy Zeroed*” and click next.

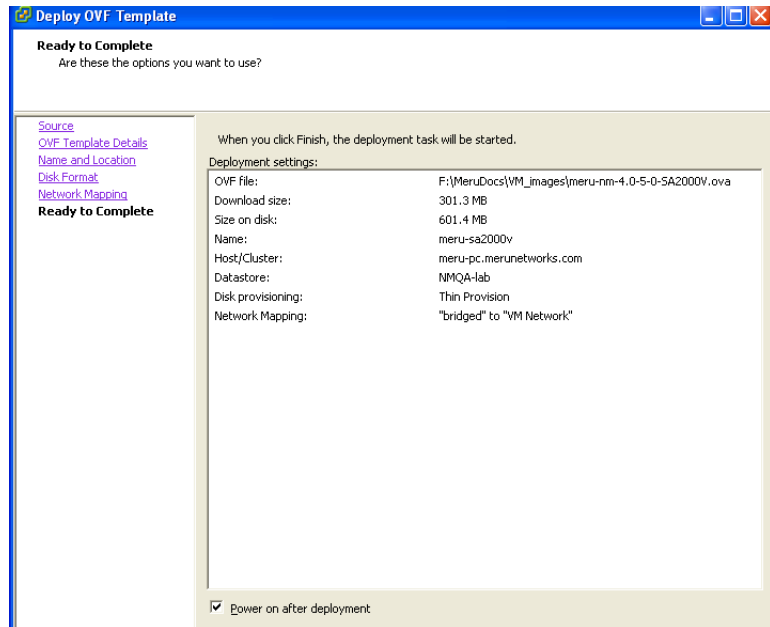
8. Click *Next* to view the Network Mapping. See [Figure 163 on page 426](#).

Figure 163: Network Mapping



9. Click *Next* to view the summary of the selections performed. Select the *Power on after deployment* option located at the lower corner of the wizard. See [Figure 164 on page 426](#).

Figure 164: Ready to Complete



10. Click *Finish* to launch NM. The time taken to launch NM will be approximately 15 minutes.

After the Fortinet services have started, login to the VMware console and verify the `sh nms` command output.

Create Virtual FortiWLM using .vmx and .vmdk file

Following are the steps to create a virtual FortiWLM using **.vmx** and **.vmdk** file.

- [“Verify the Block Size of the datastore properties” on page 427](#)
- [“NMVMdatastore Properties - Block Size” on page 428](#)
- [“Add a Network Card to a vSwitch” on page 435](#)
- [“Add Virtual NIC\(s\) to Forti WLM” on page 440](#)
- [“Power On the Virtual NM” on page 443](#)

Verify the Block Size of the datastore properties

By default datastores are created with default size of “1 MB” block size, which gives a maximum virtual hard drive size of 256 GB.

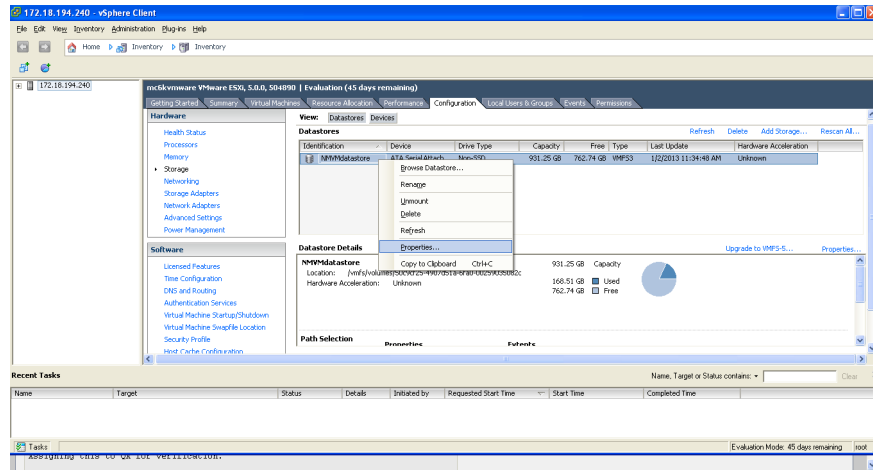
Since our virtual NM instance is almost similar to SA2000 platform in terms of system resource and hard disk capacity, which demands a minimum of 500G virtual hard disk space. In order to ensure 500G virtual hard drive space, we insist to create a datastore of block size “2MB” size.

Here is a quick reference of what block size you can choose and what the A maximum virtual hard drive that will give you:

Block Size	Max VHD size
1MB	256GB
2MB	512GB
4MB	1TB
8MB	2TB

1. From the *Hardware* section of the *Configuration* tab, select the *Storage* option.
2. In the *Datastores* section, perform a right click and select the *Properties* option of the *NMVMdatastore*. See [Figure 165 on page 428](#).

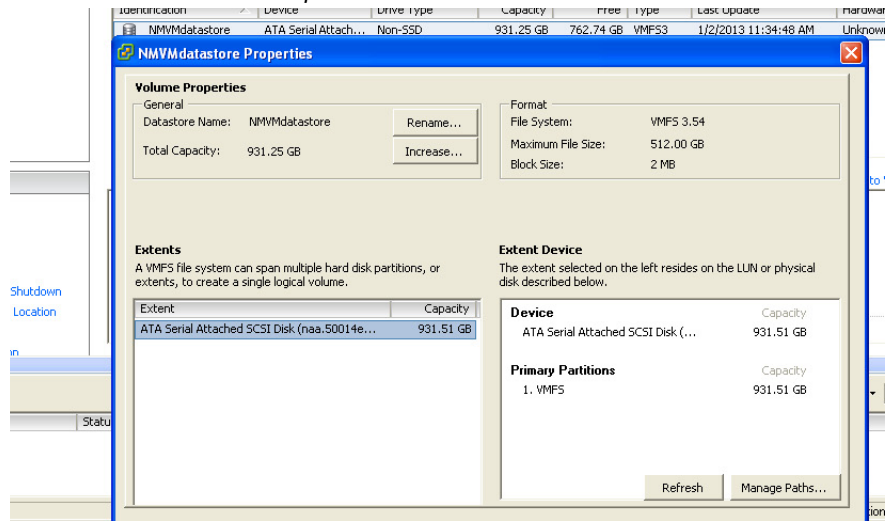
Figure 165: NMVMdatastore - Properties



3. The **Block Size** of the datastore must be **2MB**; in the **Format** section of the **NMVMdatastore Properties** screen

[Figure 166 on page 428](#) illustrates the **NMVMdatastore Properties - Block Size**.

Figure 166: NMVMdatastore Properties - Block Size



The 2MB block size limitation exists only on VMFS-3 datastore. In VMFS-5, a unified 1 MB block size is used, which is no longer configurable.

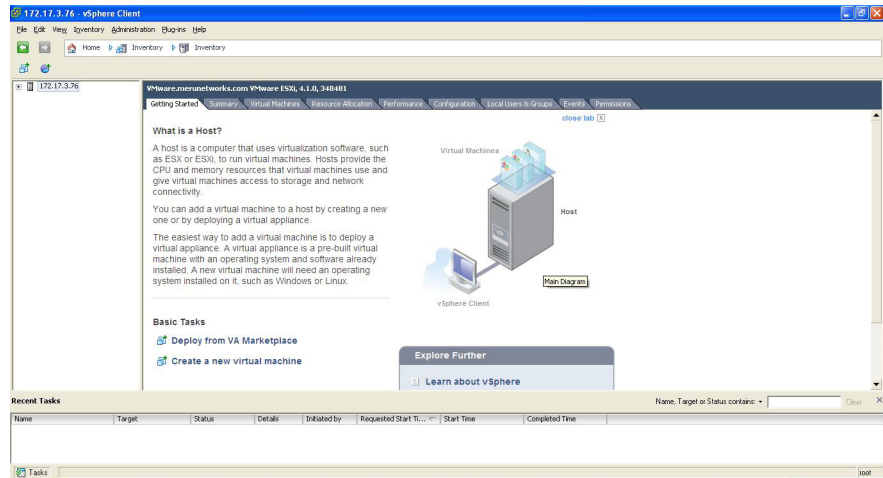
Add a Virtual FortiWLM using vSphere Client

1. Open a *vSphere Client*.
2. The *vSphere Client* displays the following:
 - **Getting Started** section displaying the below mentioned tabs:
 - Summary
 - Virtual Machines
 - Resource Allocation
 - Performance
 - Configuration
 - Local Users & Groups
 - Events
 - Permissions

The *IP Address* panel displays the *IP Address* of the host machine.

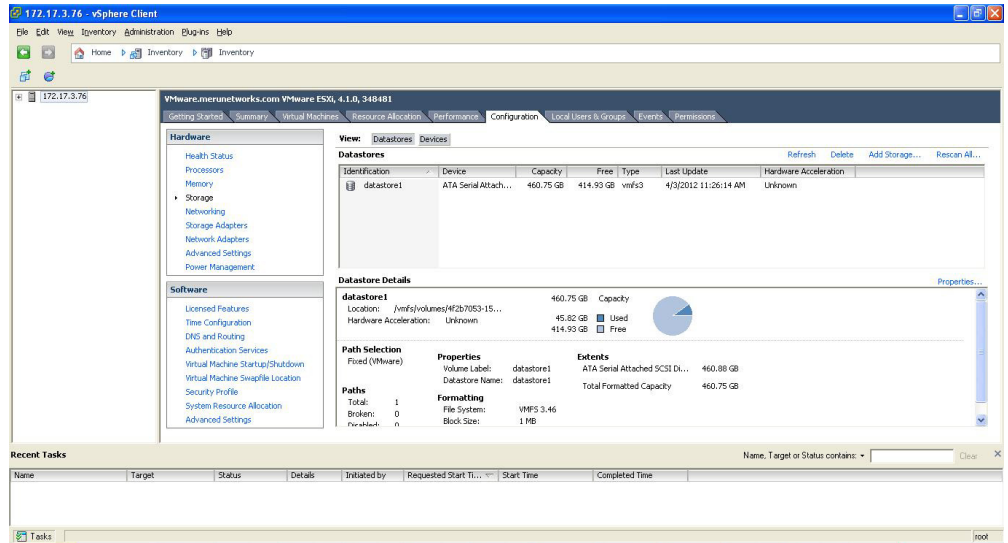
Figure 167 on page 429 illustrates the *vSphere Client*.

Figure 167: vSphere Client



3. Select the *IP Address* of the host machine followed by selecting the *Configuration* tab.
Figure 168 on page 430 illustrates the *Configuration* tab.

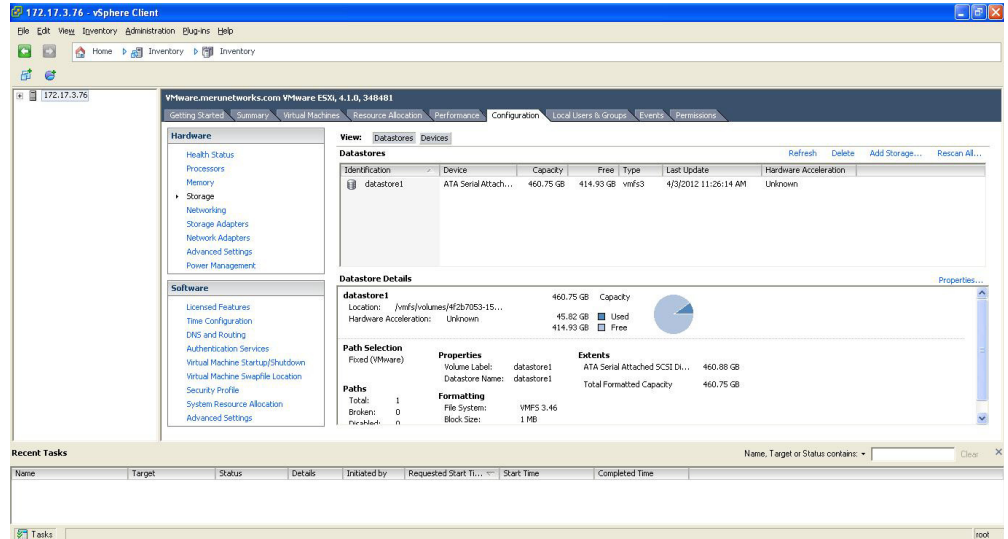
Figure 168: Configuration tab



4. The *Configuration* tab consists of the following sections:
 - Hardware
 - Software
 - View
 - Datastore Details
5. In *Hardware* section of the *Configuration* tab, select the *Storage* option to define the *Data Store(s)*.

Figure 168 on page 430 illustrates the *Configuration* tab.

Figure 169: Data Store(s)



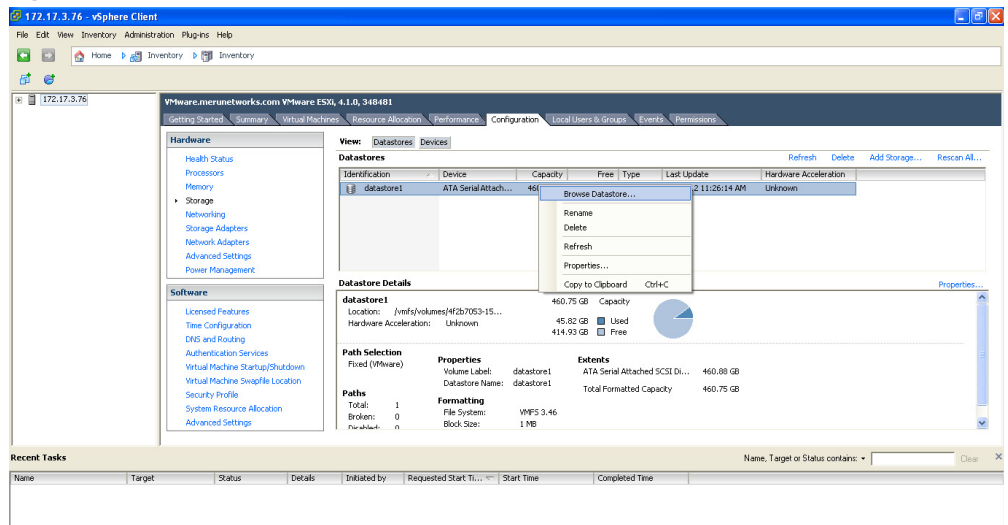
6. Select the *datastore1*.

Figure 169 on page 431 illustrates the Data Store(s).

7. Perform a right click on the *datastore1* followed by choosing the *Brows Datastore* option.

Figure 170 on page 431 illustrates the Browse Datastore.

Figure 170: Browse Datastore



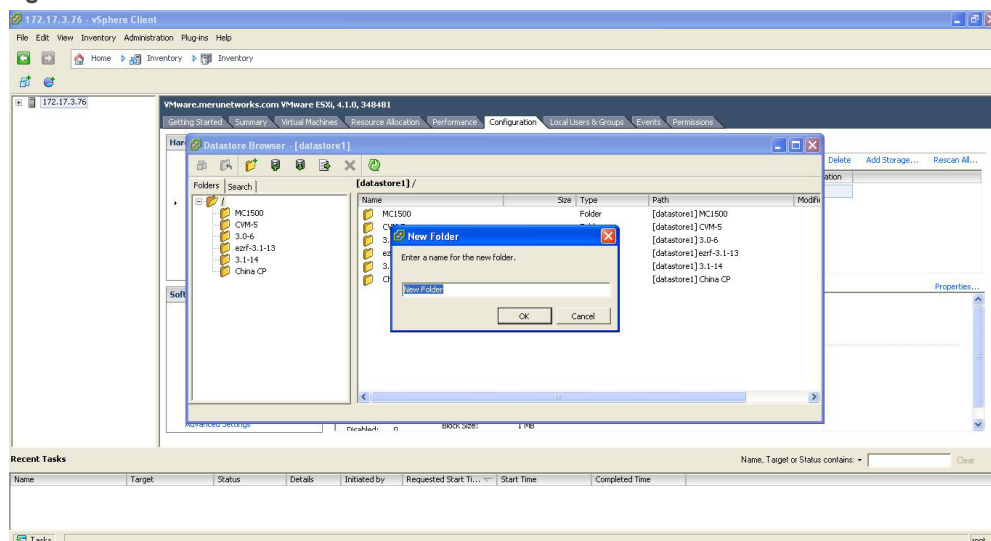
8. In the *Datastore Browser [datastore1]* wizard, select *Create a New Folder* option on the *Datastore Browser [datastore1]* wizard.

9. In the *New Folder* wizard, provide a name for the folder created.

For Example: *FortiWLM-6.1-14-SA2000-V*

Figure 171 on page 432 illustrates the *New Folder* screen.

Figure 171: New Folder



10. Before you create a folder, download the following files from the FTP server to the local hard disk.

- FortiWLM-6.1-14-SA2000V-2048.img
- FortiWLM-6.1-14-SA2000V.vmdk
- FortiWLM-6.1-14-SA2000V.vmx
- vdisk_SA2000V.vmdk

11. Select the created folder *FortiWLM-6.1-14-SA2000-V* and upload the below mentioned files that are downloaded from FTP server to the local hard disk.

Figure 172 on page 433 illustrates an *Upload File* screen.

- FortiWLM-6.1-14-SA2000V-2048.img
- FortiWLM-6.1-14-SA2000V.vmdk
- FortiWLM-6.1-14-SA2000V.vmx
- vdisk_SA2000V.vmdk

Figure 172: Upload File

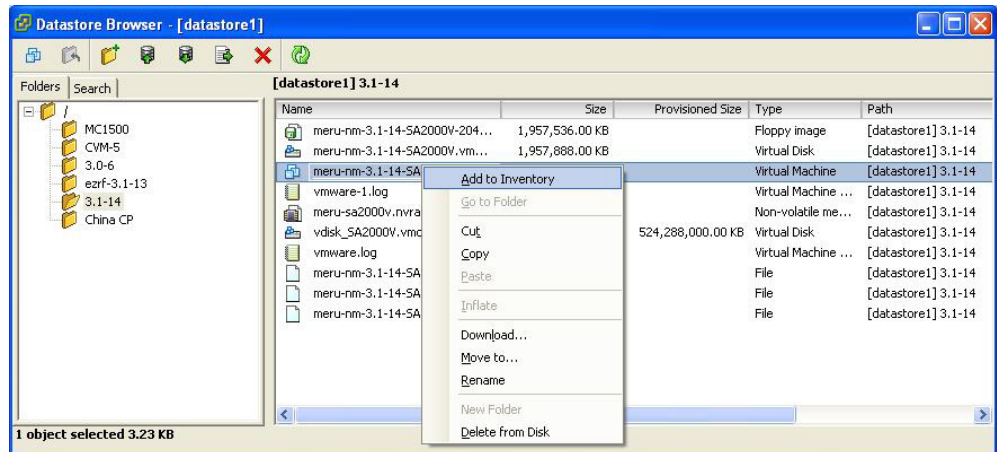


12. The created folder with the above mentioned files are now saved in .vmx format.

13. Perform a right click on the folder *FortiWLM-6.1-14-SA2000-V.vmx* and select *Add to Inventory* option.

Figure 173 on page 433 illustrates the *Add to Inventory* screen.

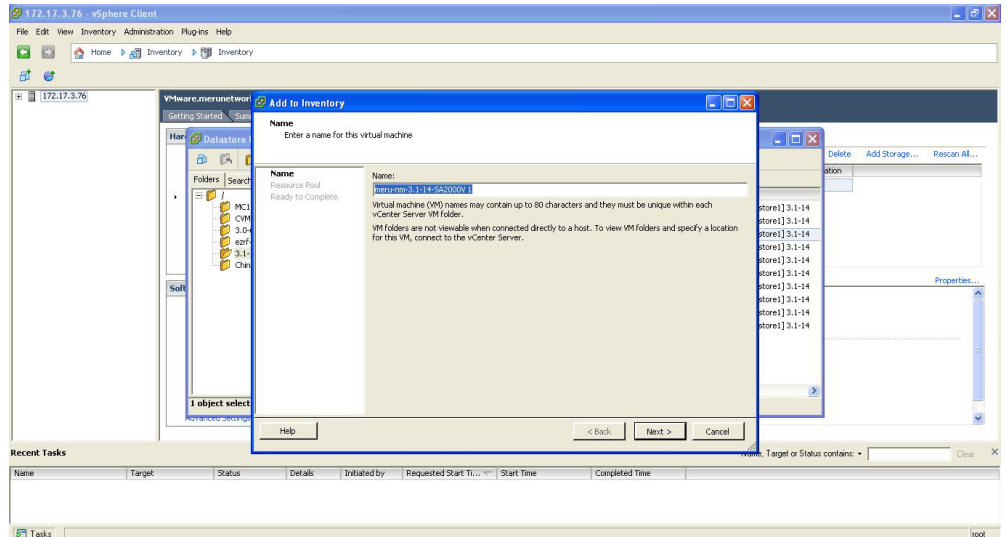
Figure 173: Add to Inventory



14. In the *Add to Inventory* wizard, provide the NM name.

Figure 174 on page 434 illustrates the *Add to Inventory - Name* screen.

Figure 174: Add to Inventory - Name



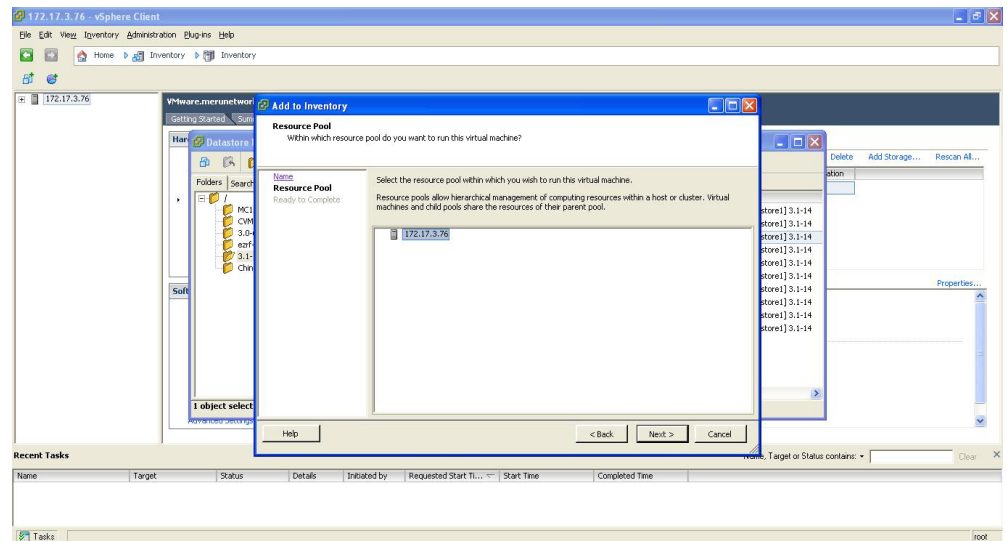
15. Select the *Next* option.

16. The *Resource Pool* screen of the *Add to Inventory* displays an IP address of the host machine.

[Figure 175 on page 434](#) illustrates the *Resource Pool - Host Machine* screen

17. Select the *Host Machine* followed by selecting the *Next* option.

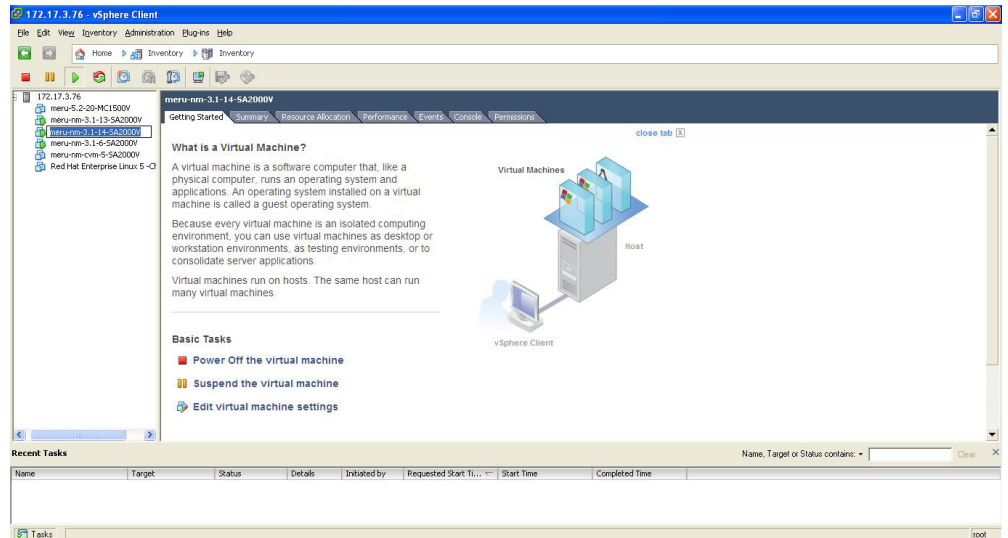
Figure 175: Resource Pool - Host Machine



18. Select *Finish*. The *Virtual Machine (VM)* is now created and is added to the selected Host's Inventory.

[Figure 176 on page 435](#) illustrates the *Virtual Machine on Host's Inventory* screen.

Figure 176: Virtual Machine on Host's Inventory



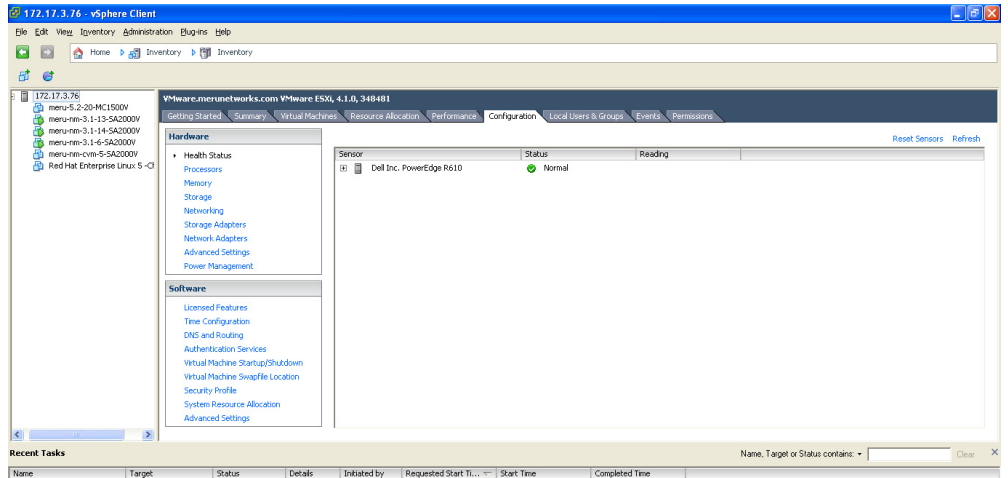
Add a Network Card to a vSwitch

1. Open a *vSphere Client*.
2. The *vSphere Client* displays the following:
 - *Getting Started* section displaying the below mentioned tabs:
 - Summary
 - Virtual Machines
 - Resource Allocation
 - Performance
 - Configuration
 - Local Users & Groups
 - Events
 - Permissions
 - *IP Address* panel displaying the *IP Address* of the host machine.
3. Select the *IP Address* of the host machine displayed on the *IP Address* panel followed by selecting the *Configuration* tab.
4. The *Configuration* tab consists of the following sections:
 - Hardware
 - Software

- View
- Datastore Details.

Figure 177 on page 436 illustrates the *vSphere Client - IP Address* screen.

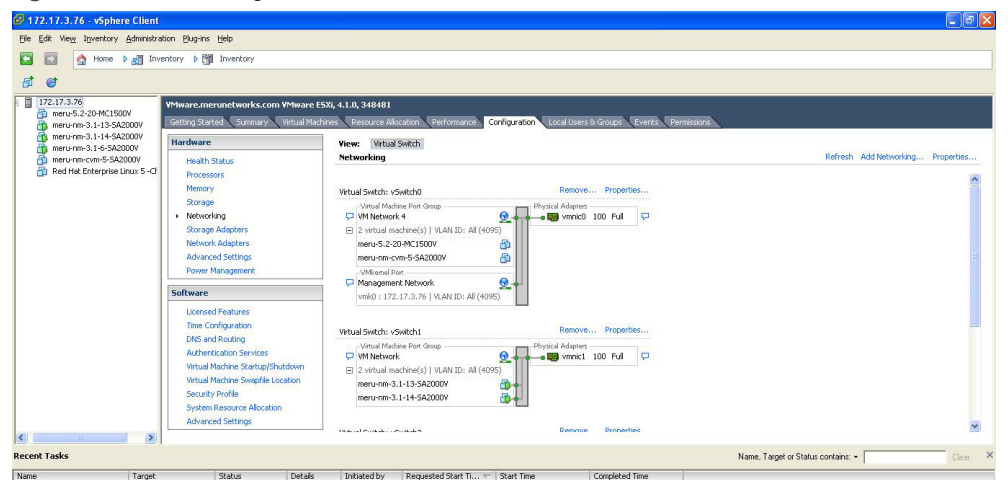
Figure 177: vSphere Client - IP Address



- From the *Hardware* section of the *Configuration* tab, select the *Networking* option.

Figure 178 on page 436 illustrates the *Networking* screen.

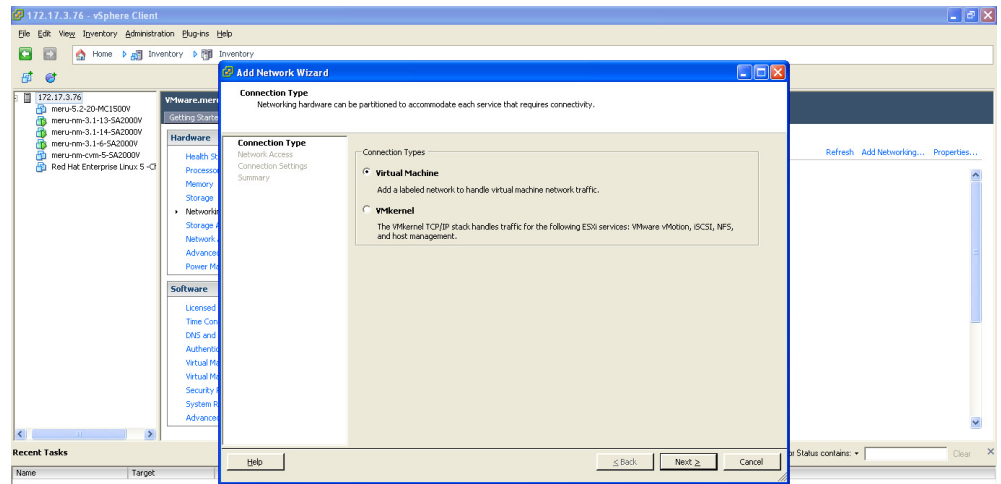
Figure 178: Networking



- The *Networking* screen displays the existing *Network*.
- Apart from the existing *Network*, the following options is also displayed towards the right side corner:
 - Refresh

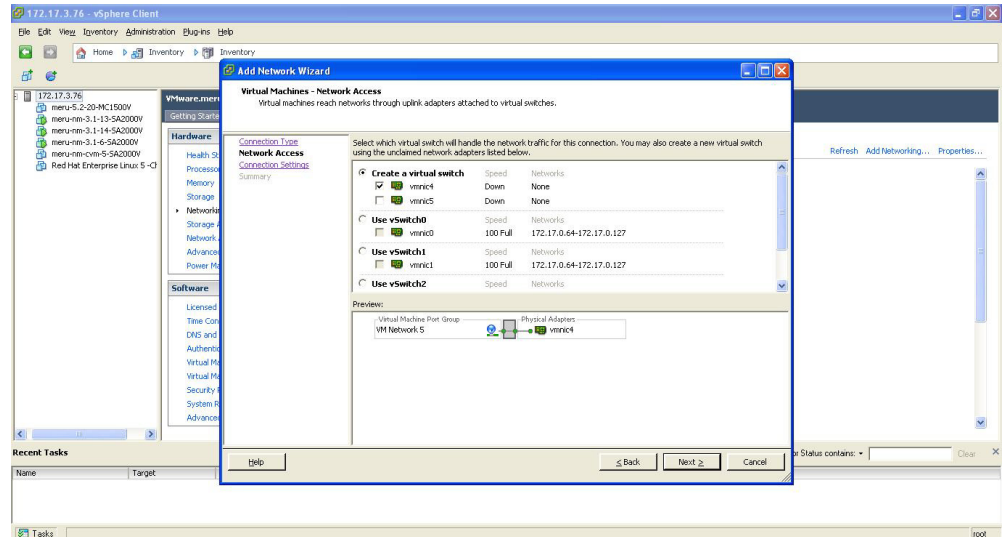
- Add Networking
 - Properties
8. Select the *Add Networking* option.
9. The *Add Network* wizard provides the below connection options:
- Virtual Machine (*Figure 179 on page 437* illustrates the *Virtual Machine* screen)
 - VMkernel

Figure 179: Virtual Machine



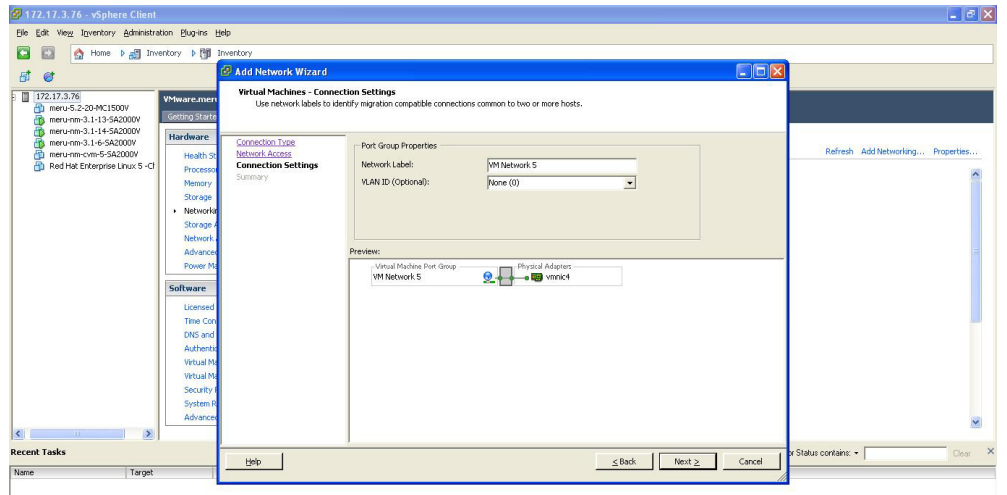
10. Select the *Virtual Machine* as the Connection type.
11. Select *Next*.
12. The *Virtual Machines - Network Access* screen provides the following options: (*Figure 180 on page 438* illustrates the *Virtual Machines - Network Access* screen)
- Create a virtual switch
 - Use vSwitch0
 - Use vSwitch1
 - Use vSwitch2

Figure 180: Virtual Machines - Network Access



13. From the above mentioned options, select the *Create a virtual switch* as the Network Access option. (Figure 180 on page 438 illustrates the *Virtual Machines - Connection Settings* screen)
14. The *Create a virtual switch* provides an option to select the card. Select the desired card.
15. Select *Next*. The *Virtual Machines - Connection Settings* screen is displayed.

Figure 181: Virtual Machines - Connection Settings



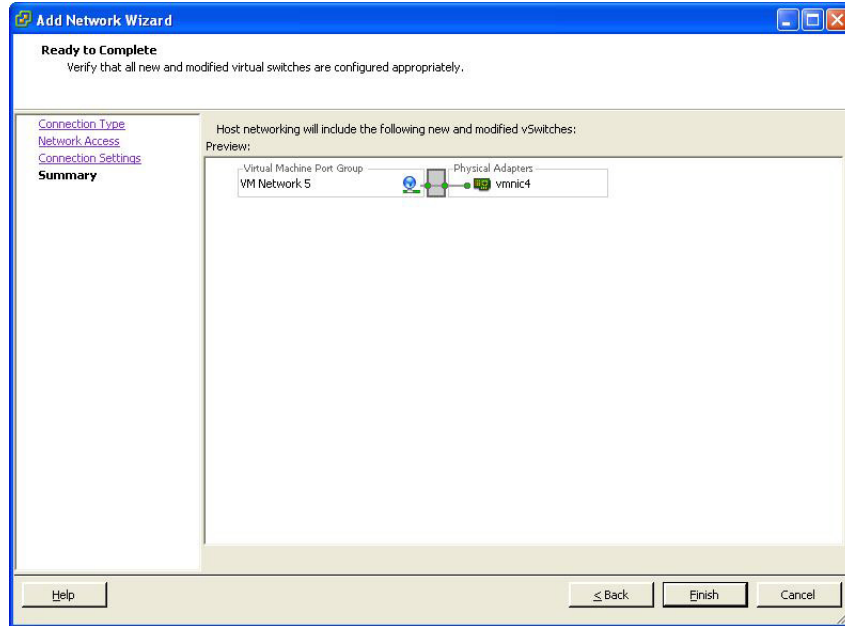
16. The *Virtual Machines - Connection Settings* screen provides the following options:
 - *Network Label*: Provide a name as a *Network Label*.

- *VLAN ID (Optional)*: Select *ALL (4096)* from the drop-down list to enable VLAN support on the Network Card.

17. Select *Next*.

18. In the *Ready to Complete* screen, select *Finish*. (*Figure 182 on page 439* illustrates the *Ready to Complete* screen)

Figure 182: Ready to Complete

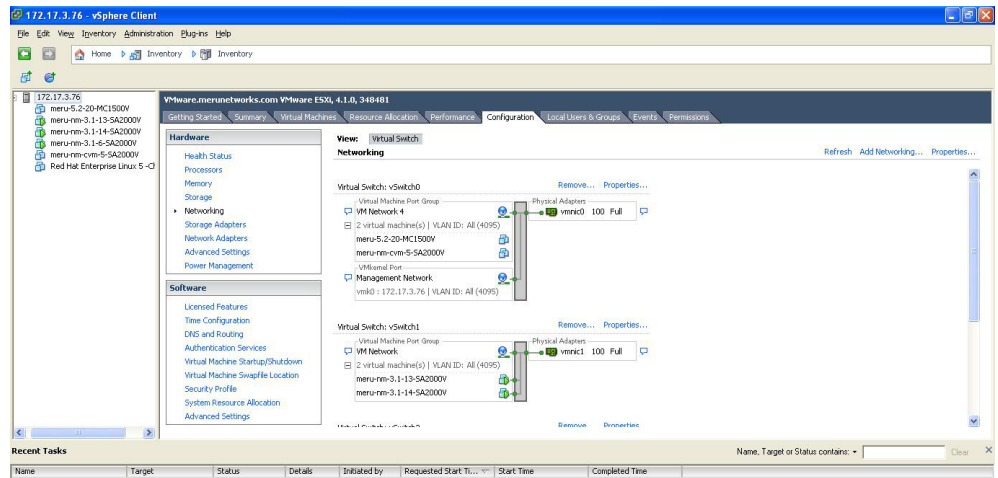


19. The *Network Adaptor* is now added.

20. To verify the addition of *Network Adaptor*, select the *Networking* link on the *Configuration* tab.

21. In the *Networking* link on the *Configuration* tab, select the *Properties* option of the recently added virtual switch (*Figure 183 on page 440* illustrates the *Networking* link on the *Configuration* tab)

Figure 183: Networking link on the Configuration tab



Add Virtual NIC(s) to Forti WLM

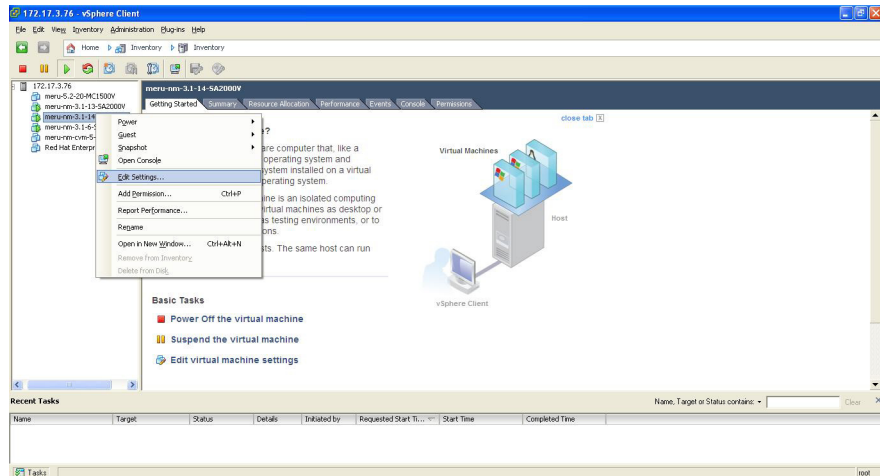
Once the *NM* is added to the inventory, the *Network Card* must be assigned to the *NM*.

1. The *vSphere Client* displays the following:

- *Getting Started* section displaying the below mentioned tabs:
 - Summary
 - Virtual Machines
 - Resource Allocation
 - Performance
 - Configuration
 - Local Users & Groups
 - Events
 - Permissions
- *IP Address* panel displaying the *IP Address* of the host machine.

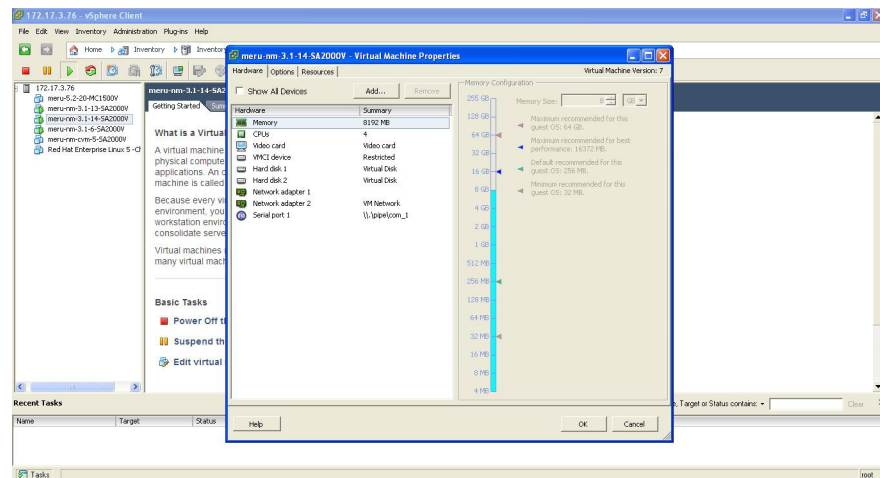
2. Select the *FortiWLM* displayed on the *IP Address* panel from the Inventory list. Perform a right click and select *Edit Settings*. ([Figure 184 on page 441](#) illustrates the *FortiWLM Instance* screen.)

Figure 184: FortiWLM Instance



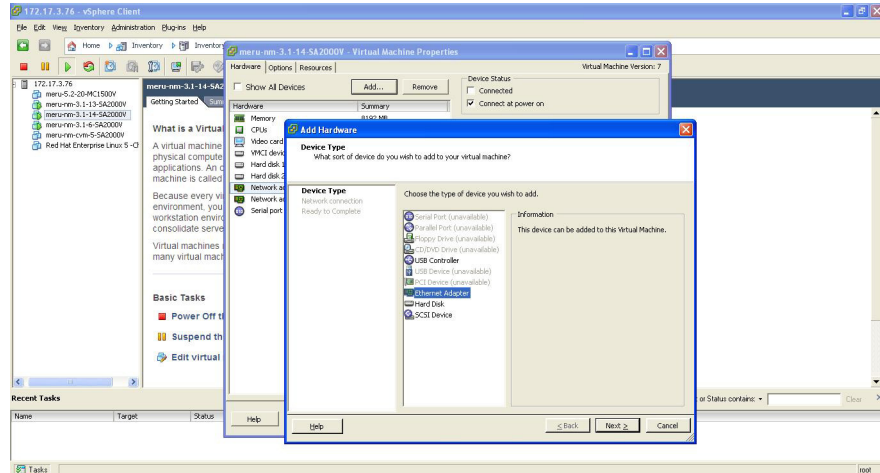
3. In *Hardware* tab on the *FortiWLM-6.1-14-SA2000-V - Virtual Machine Properties* wizard, select *Add*. (See [Figure 185 on page 441](#) illustrates the *FortiWLM-6.1-14-SA2000-V - Virtual Machine Properties* wizard)

Figure 185: FortiWLM-6.1-14-SA2000-V - Virtual Machine Properties



4. In the *Add Hardware* wizard select the *Ethernet Adapter*. ([Figure 186 on page 442](#) illustrates the *Add Hardware* screen.)
5. Select *Next*.

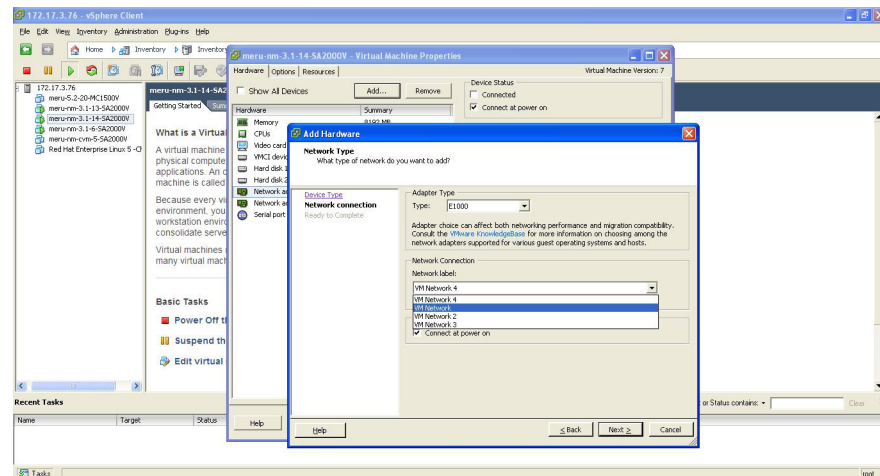
Figure 186: Add Hardware



6. In the *Add Hardware - Network Type* screen, select the following options on the *Network Type* screen.

- *Adaptor Type* - Select the *Adaptor Type* as *E1000*.
 - *Network Connection* - Select the *Network Connection* as *Network Label*.
- [Figure 187 on page 442](#) illustrates the *Network Type* screen.

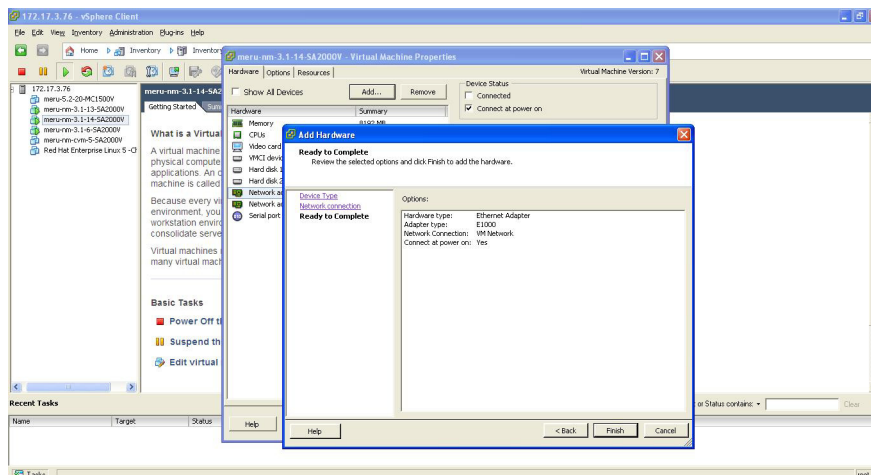
Figure 187: Network Type



7. Select *Next* to navigate to subsequent screens.

8. Lastly, select *Finish* to set up the NM. ([Figure 188 on page 443](#) illustrates the *Ready to Complete - NM* screen.)

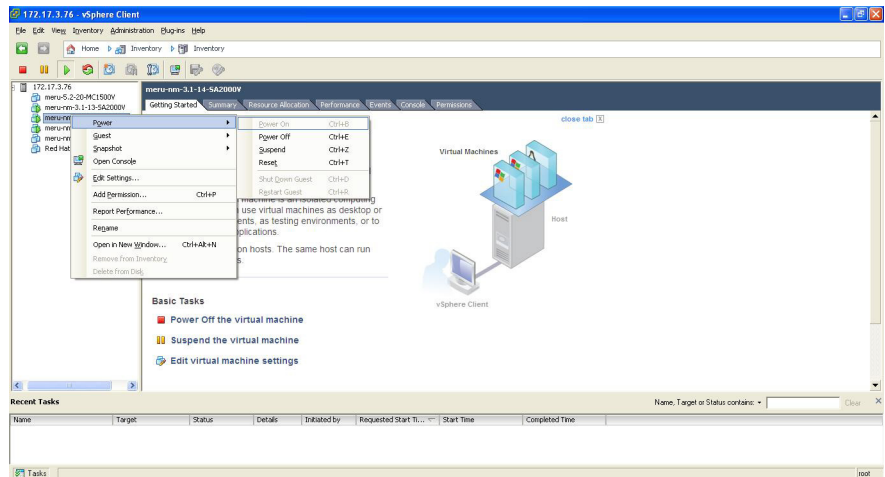
Figure 188: *Ready to Complete - NM*



Power On the Virtual NM

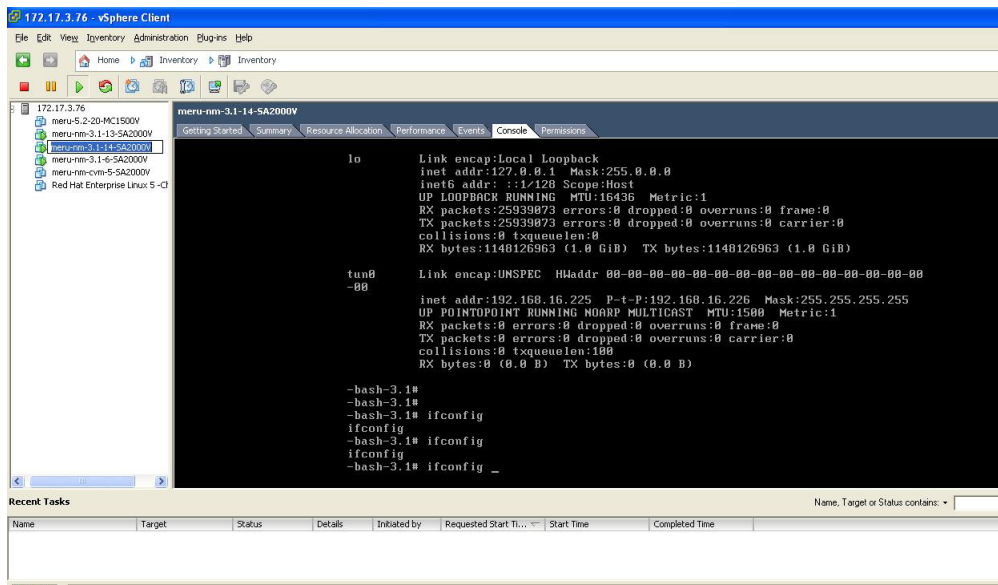
1. The *vSphere Client* displays the following:
 - *Getting Started* section displaying the below mentioned tabs:
 - Summary
 - Virtual Machines
 - Resource Allocation
 - Performance
 - Configuration
 - Local Users & Groups
 - Events
 - Permissions
 - *IP Address* panel displaying the *IP Address* of the host machine.
2. Select the *FortiWLM* displayed on the *IP Address* panel from the Inventory list.
3. Perform a right click and select *Power* followed by *Power On* option to power on the NM. (*Figure 189 on page 444* illustrates the *FortiWLM Instance* screen.)

Figure 189: FortiWLM Instance



4. In order to access the console of the NM, select the NM from the inventory and click the *Console* tab. (Figure 190 on page 444 illustrates the FortiWLM Console screen.)

Figure 190: FortiWLM Console



Troubleshooting FortiWLM-Virtual Edition

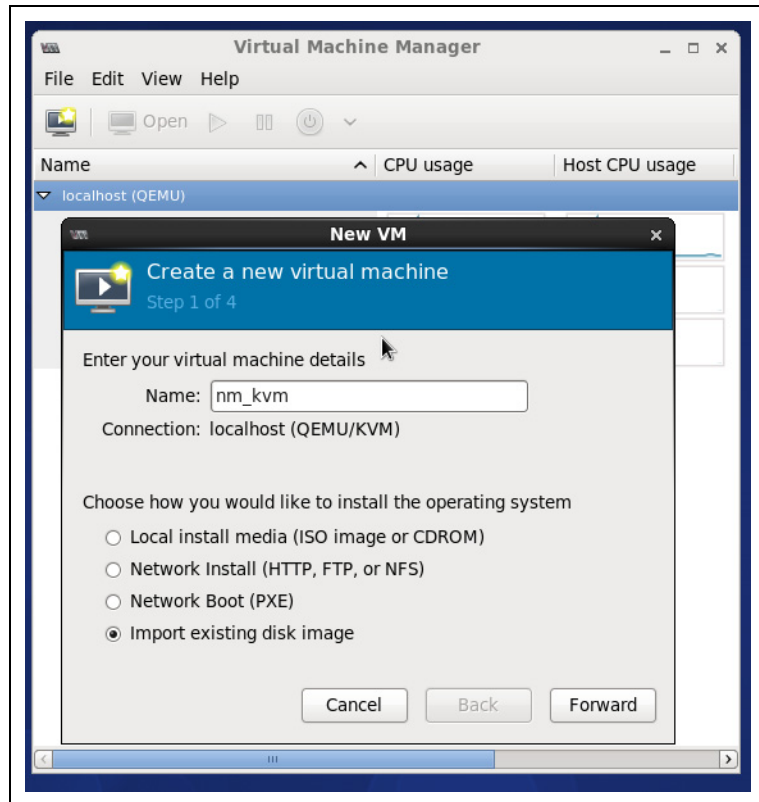
The following table lists the common problems faced after installing *E(z)RF-Virtual Edition* with potential solutions. If your problem does not appear in the table or the solution provided doesn't remedy the situation, contact *Fortinet Technical Support* for further assistance.

Message	Possible Cause and Solution
Unable to connect to MKS: Virtual machine config file doesn't exist	<p>This message can appear due to one of the following problems:</p> <p>The <i>vmx</i> files found missing in the datastore. Only <i>img</i>, <i>vmdf</i> and <i>vswp</i> files were existing.</p> <p>Solution:</p> <p>Restart the management services.</p> <p>Create another instance and restore the backup taken from the previous instance.</p>

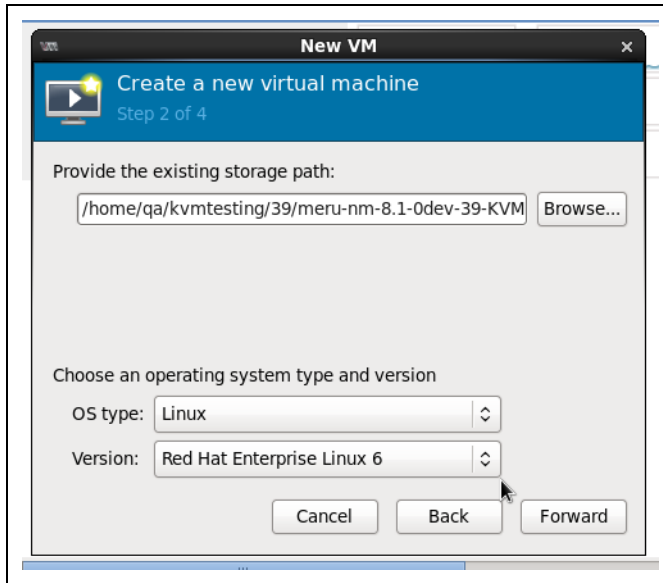
Support for KVM Virtualization

Network Manager virtual image can be installed in KVM-53 virtual server. The following are the steps to set up a virtual server and install Network Manager.

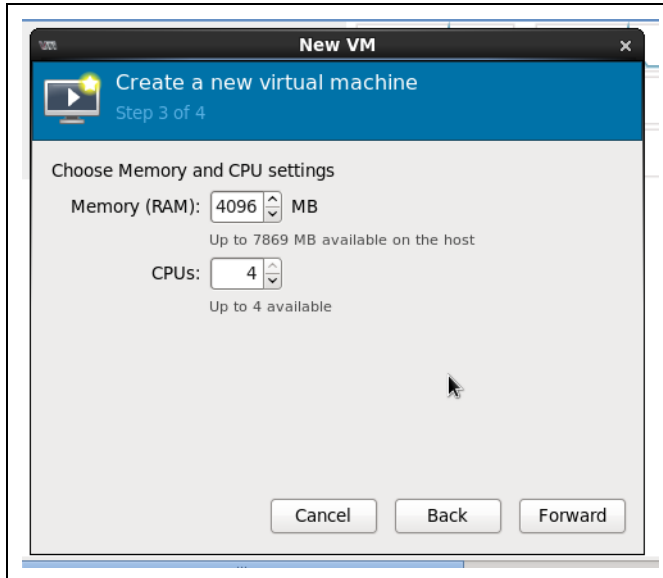
1. Create a new virtual machine. Enter a name of the VM and select Import existing disk image.



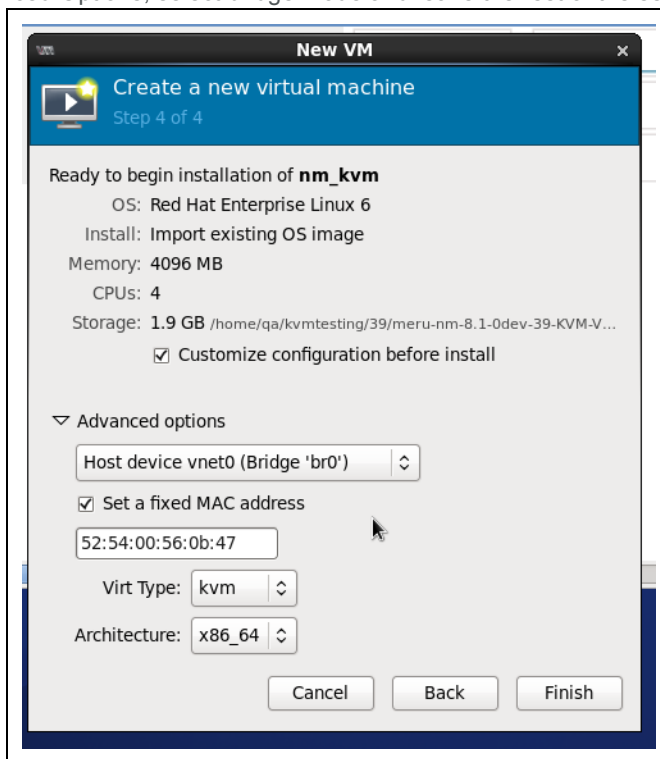
2. Select the image file (.tar), set OS type to Linux, and Version to Red Hat Enterprise Linux 6.



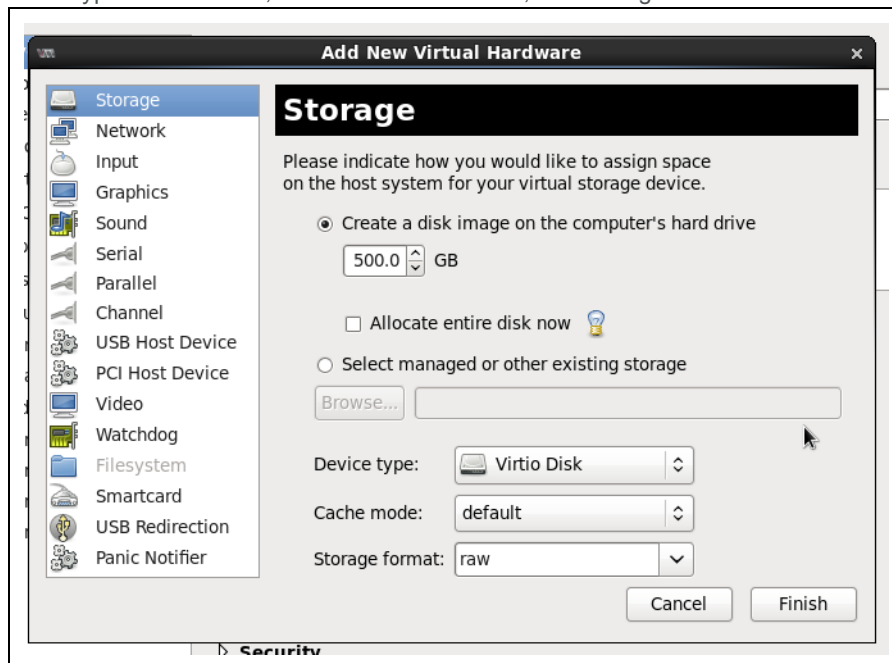
3. Specify RAM size and number of CPUs



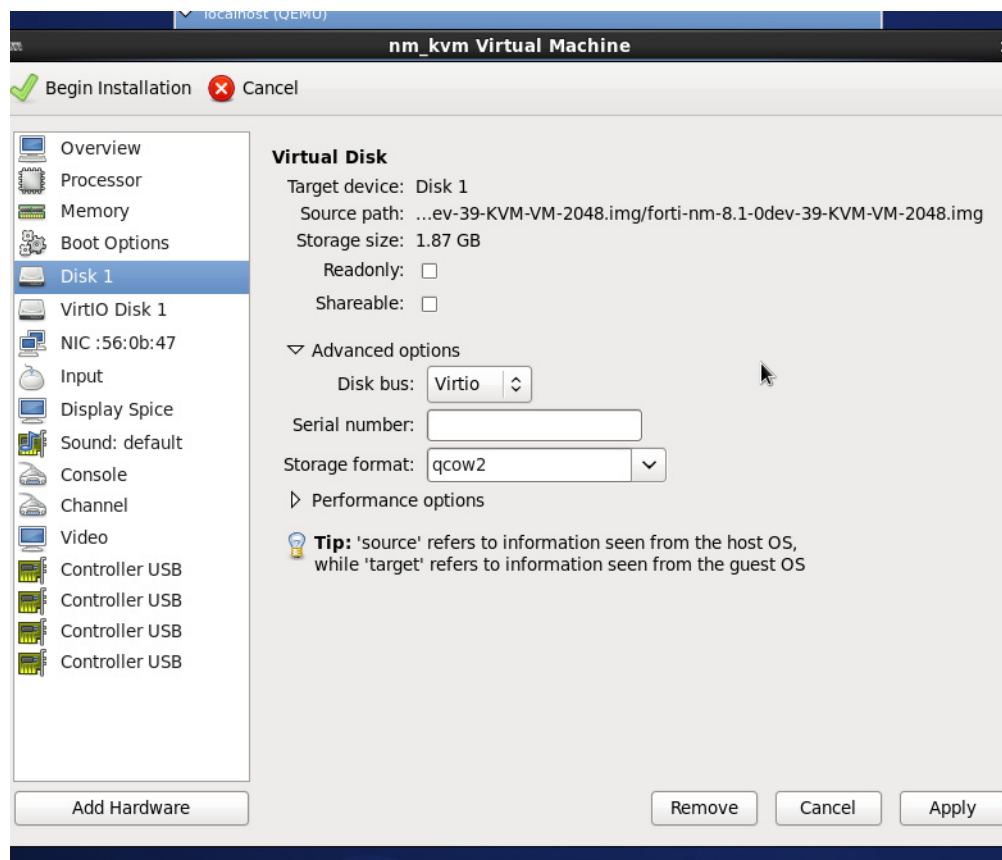
4. In the Advanced Options, select bridge mode and leave the rest of the settings in default.



5. Create a hard disk with minimum 500 GB and deselect Allocate entire disk now. Select Device type to Virtio Disk, Cache mode to default, and storage format to raw.



6. Configure hard disk settings, set the Disk bus to Virtio and Storage format to qcow2



7. Now, run this virtual machine.

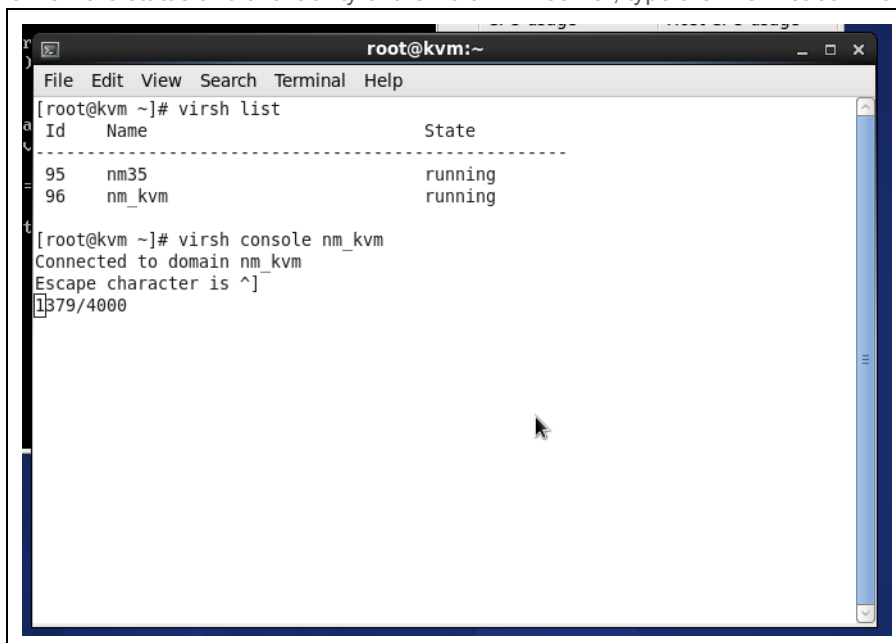
```
SeaBIOS (version seabios-0.6.1.2-30.el6)
Machine UUID 63d929dd-f8bf-af57-4502-27a3f3346e03

gPXE (http://etherboot.org) - 00:03.0 CA00 PCI2.10 PnP BBS PMMDFE0e10 CA00

Booting from Hard Disk...
GRUB Loading stage1.5.

GRUB loading, please wait...
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
-
```

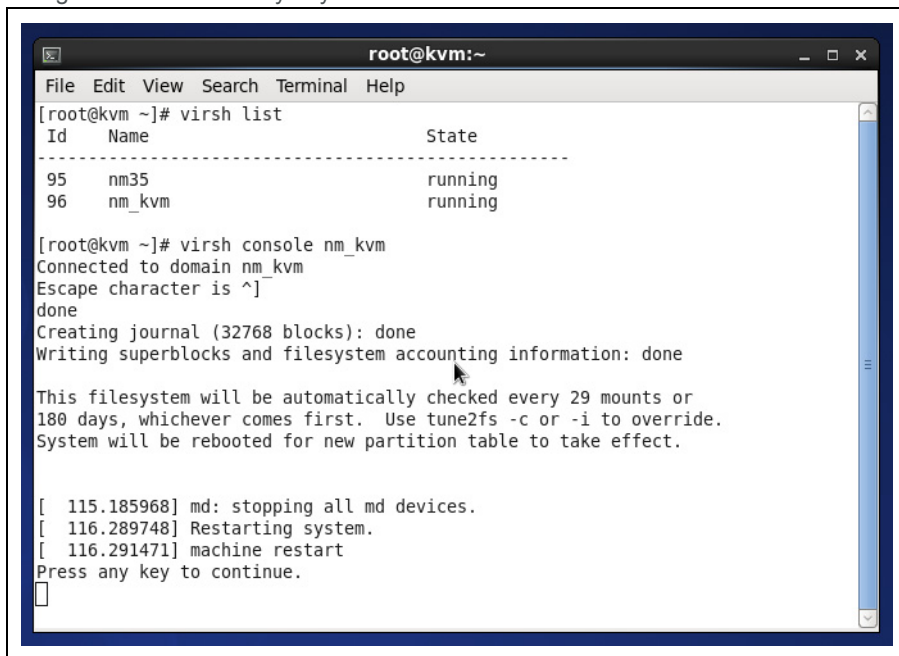
8. To view the status and availability of the FortiWLM server, type the virsh list command.



```
root@kvm:~
File Edit View Search Terminal Help
[root@kvm ~]# virsh list
  Id    Name         State
  ----  -
  95    nm35          running
  96    nm_kvm        running

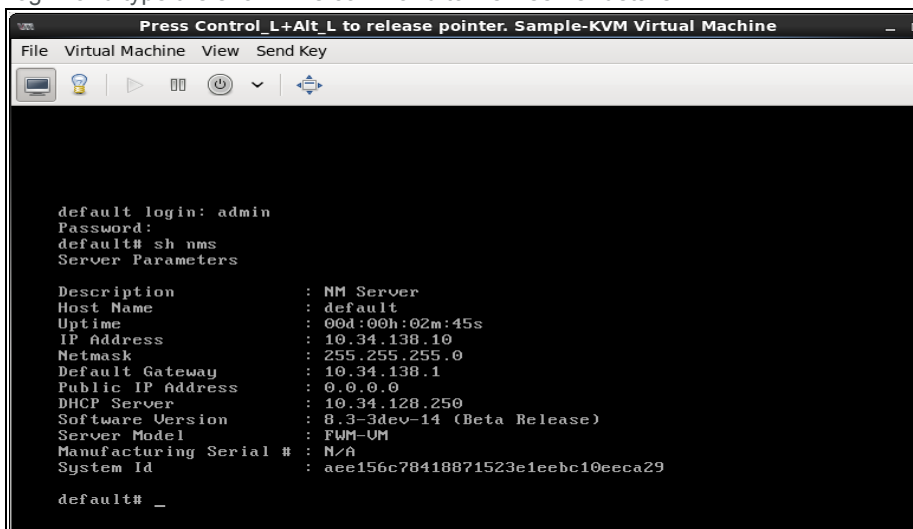
[root@kvm ~]# virsh console nm_kvm
Connected to domain nm_kvm
Escape character is ^[
1379/4000
```

9. When complete, this command will list the newly created virtual machine for the Network Manager server. Press any key to continue and boot into the FortiWLM server.



```
root@kvm:~  
File Edit View Search Terminal Help  
[root@kvm ~]# virsh list  
-----  
Id      Name      State  
-----  
95      nm35      running  
96      nm_kvm    running  
  
[root@kvm ~]# virsh console nm_kvm  
Connected to domain nm_kvm  
Escape character is ^]  
done  
Creating journal (32768 blocks): done  
Writing superblocks and filesystem accounting information: done  
  
This filesystem will be automatically checked every 29 mounts or  
180 days, whichever comes first. Use tune2fs -c or -i to override.  
System will be rebooted for new partition table to take effect.  
  
[ 115.185968] md: stopping all md devices.  
[ 116.289748] Restarting system.  
[ 116.291471] machine restart  
Press any key to continue.  
[
```

10. Log in and type the show nms command to view server details.

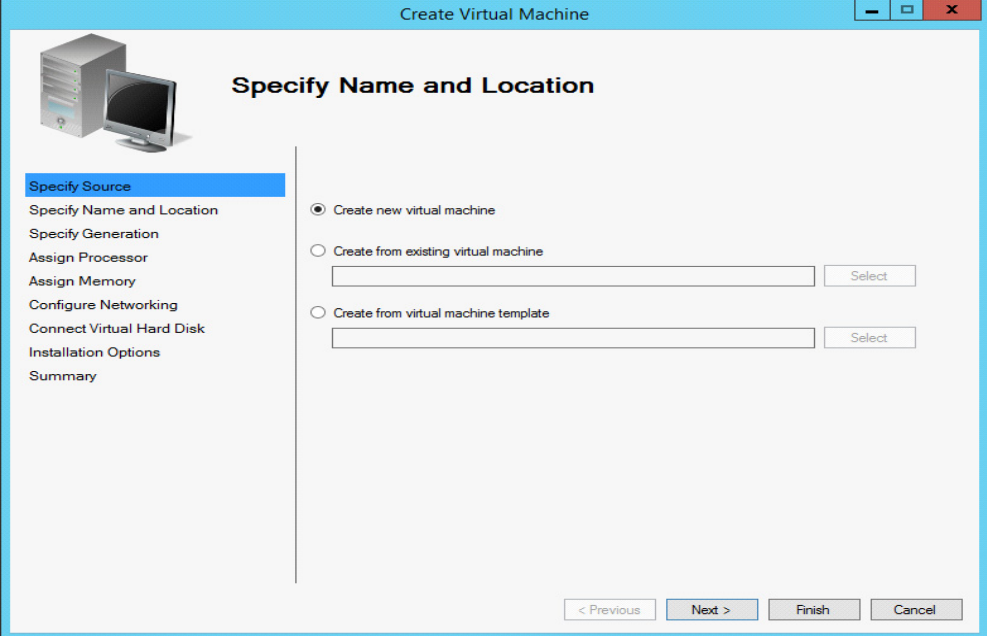


```
Press Control_L+Alt_L to release pointer. Sample-KVM Virtual Machine  
File Virtual Machine View Send Key  
[Icons]  
  
default login: admin  
Password:  
default# sh nms  
Server Parameters  
  
Description      : NM Server  
Host Name        : default  
Uptime           : 00d:00h:02m:45s  
IP Address       : 10.34.138.10  
Netmask          : 255.255.255.0  
Default Gateway  : 10.34.138.1  
Public IP Address : 0.0.0.0  
DHCP Server      : 10.34.128.250  
Software Version  : 8.3-3dev-14 (Beta Release)  
Server Model     : FWM-UM  
Manufacturing Serial # : N/A  
System Id        : ace156c78418871523e1eebc10eeeca29  
  
default# _
```


Support for Hyper-V Virtualization

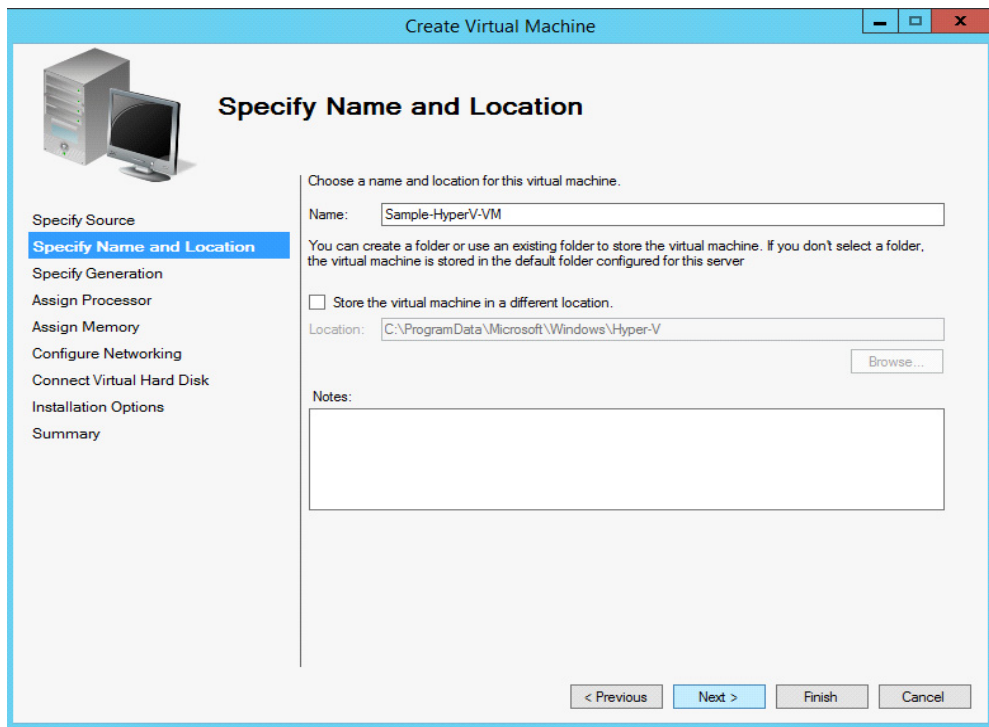
Open Hyper-V Manager. Right click on Hyper-V Server and select Create New VM to open the New Virtual Machine Wizard.

1. Click the **Next** button on the **Specify Source** page to create a new Virtual Machine.



The screenshot shows the 'Create Virtual Machine' wizard window. The title bar reads 'Create Virtual Machine'. On the left, there is a list of steps: 'Specify Source' (highlighted in blue), 'Specify Name and Location', 'Specify Generation', 'Assign Processor', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. Above the list is an icon of a server and a monitor. The main area is titled 'Specify Name and Location'. It contains three radio button options: 'Create new virtual machine' (selected), 'Create from existing virtual machine', and 'Create from virtual machine template'. The second and third options have text input fields and 'Select' buttons. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

2. Enter the **Name** and select the **Location** by clicking on **Browse** button to store the Virtual Machine.



The screenshot shows the 'Create Virtual Machine' wizard window. The title bar is blue with the text 'Create Virtual Machine' and standard window controls. On the left is a vertical sidebar with icons and a list of steps: 'Specify Source', 'Specify Name and Location' (highlighted in blue), 'Specify Generation', 'Assign Processor', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area has a light gray background. At the top left of the main area is an icon of a server and monitor. To its right is the title 'Specify Name and Location'. Below this, the text 'Choose a name and location for this virtual machine.' is followed by a text box labeled 'Name:' containing 'Sample-HyperV-VM'. Below that is a paragraph: 'You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server'. This is followed by a checkbox labeled 'Store the virtual machine in a different location.' which is unchecked. Below the checkbox is a text box labeled 'Location:' containing 'C:\ProgramData\Microsoft\Windows\Hyper-V'. To the right of this text box is a 'Browse...' button. Below the 'Location' section is a 'Notes:' label followed by a large empty text area. At the bottom right of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Create Virtual Machine

Specify Name and Location

Specify Source
Specify Name and Location
Specify Generation
Assign Processor
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

Choose a name and location for this virtual machine.

Name: Sample-HyperV-VM

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server

☐ Store the virtual machine in a different location.

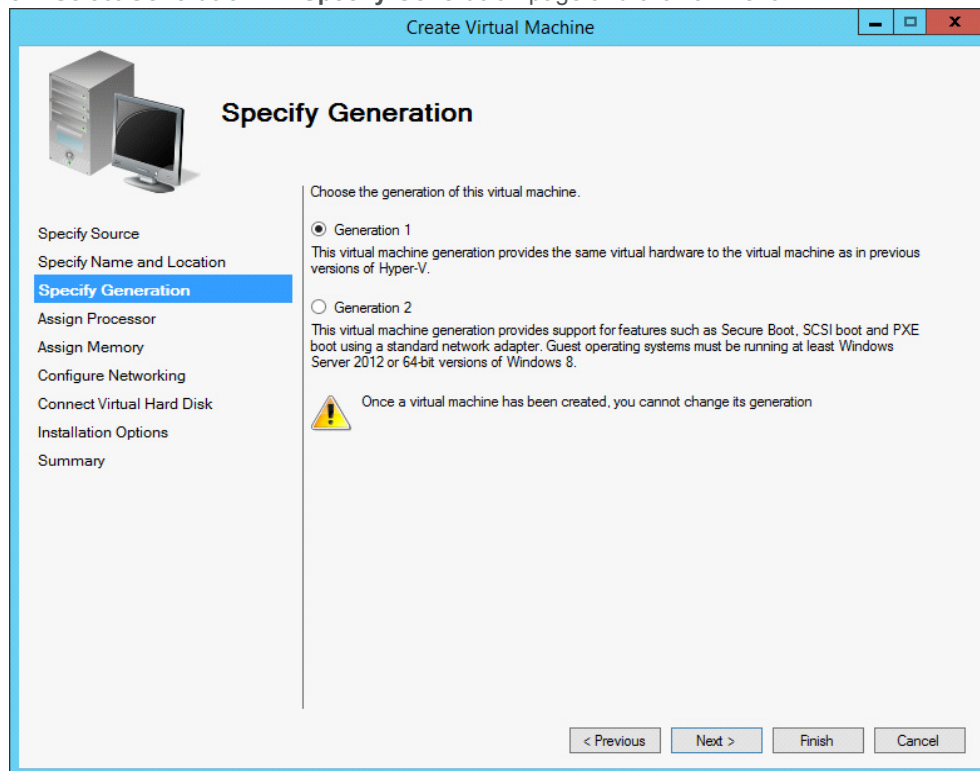
Location: C:\ProgramData\Microsoft\Windows\Hyper-V

Browse...

Notes:

< Previous Next > Finish Cancel

3. Select **Generation1** in **Specify Generation** page and click on **Next**.



The screenshot shows the 'Specify Generation' page of the 'Create Virtual Machine' wizard. The window title is 'Create Virtual Machine'. On the left, a navigation pane lists the steps: 'Specify Source', 'Specify Name and Location', 'Specify Generation' (highlighted in blue), 'Assign Processor', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. Above the list is an icon of a server and monitor. The main area is titled 'Specify Generation' and contains the instruction 'Choose the generation of this virtual machine.' There are two radio button options: 'Generation 1' (selected) and 'Generation 2'. Below 'Generation 1' is a description: 'This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.' Below 'Generation 2' is a description: 'This virtual machine generation provides support for features such as Secure Boot, SCSI boot and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.' A yellow warning triangle icon is positioned above the text 'Once a virtual machine has been created, you cannot change its generation'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.


Create Virtual Machine

Specify Generation

Choose the generation of this virtual machine.

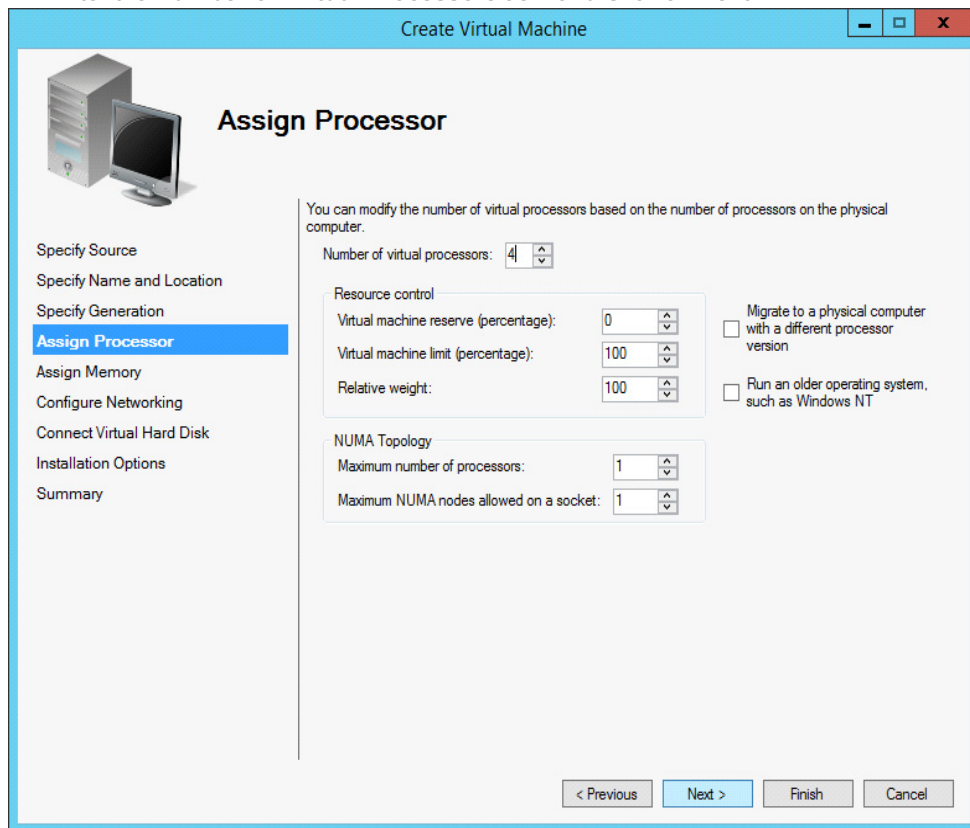
☒ Generation 1
This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

☐ Generation 2
This virtual machine generation provides support for features such as Secure Boot, SCSI boot and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.

 Once a virtual machine has been created, you cannot change its generation

< Previous Next > Finish Cancel

4. Enter the **Number of Virtual Processors** as 4 and Click on **Next**.



The screenshot shows the 'Create Virtual Machine' wizard with the 'Assign Processor' step selected. The wizard has a blue title bar and a sidebar on the left with the following steps: Specify Source, Specify Name and Location, Specify Generation, **Assign Processor** (highlighted in blue), Assign Memory, Configure Networking, Connect Virtual Hard Disk, Installation Options, and Summary. The main area is titled 'Assign Processor' and includes an icon of a server and monitor. Below the icon is a list of steps: Specify Source, Specify Name and Location, Specify Generation, **Assign Processor**, Assign Memory, Configure Networking, Connect Virtual Hard Disk, Installation Options, and Summary. The main content area contains the following text: 'You can modify the number of virtual processors based on the number of processors on the physical computer.' Below this text is a 'Number of virtual processors' field with a spinner set to 4. To the right of this field are two checkboxes: 'Migrate to a physical computer with a different processor version' and 'Run an older operating system, such as Windows NT'. Below the 'Number of virtual processors' field is a 'Resource control' section with three fields: 'Virtual machine reserve (percentage):' set to 0, 'Virtual machine limit (percentage):' set to 100, and 'Relative weight:' set to 100. Below the 'Resource control' section is a 'NUMA Topology' section with two fields: 'Maximum number of processors:' set to 1 and 'Maximum NUMA nodes allowed on a socket:' set to 1. At the bottom of the wizard are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Create Virtual Machine

Assign Processor

You can modify the number of virtual processors based on the number of processors on the physical computer.

Number of virtual processors: 4

Resource control

Virtual machine reserve (percentage): 0

Virtual machine limit (percentage): 100

Relative weight: 100

NUMA Topology

Maximum number of processors: 1

Maximum NUMA nodes allowed on a socket: 1

☐ Migrate to a physical computer with a different processor version

☐ Run an older operating system, such as Windows NT

< Previous Next > Finish Cancel

5. Enter the memory size. Recommended memory size is **4 GB (4096 MB)** and click on **Next**.

The screenshot shows the 'Create Virtual Machine' wizard with the 'Assign Memory' step selected. The left sidebar lists the steps: Specify Source, Specify Name and Location, Specify Generation, Assign Processor, **Assign Memory**, Configure Networking, Connect Virtual Hard Disk, Installation Options, and Summary. The main area is titled 'Assign Memory' and includes an icon of a computer. The instructions state: 'Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 29344 MB. To improve performance, specify more than minimum amount recommended for this operating system.' The 'Startup RAM' is set to 4096 MB and 'Max memory blocks per NUMA node (MB)' is also 4096 MB. Under 'Dynamic Memory', the 'Enable Dynamic Memory' checkbox is checked. 'Minimum RAM' is 32 MB and 'Maximum RAM' is 29344 MB. The 'Memory buffer' is set to 20%. The 'Memory weight' section has a slider set to the middle position between 'Low' and 'High'. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

Create Virtual Machine

Assign Memory

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 29344 MB. To improve performance, specify more than minimum amount recommended for this operating system.

Startup RAM: 4096 MB Max memory blocks per NUMA node (MB): 4096 MB

Dynamic Memory
You can manage the amount of memory assigned to this virtual machine dynamically within the specified range.

☒ Enable Dynamic Memory

Minimum RAM: 32 MB
Maximum RAM: 29344 MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

Memory weight
Specify how to prioritize the availability of memory for this virtual machine compared to other machines on this computer.

Low High

Specifying a lower setting for this virtual machine might prevent it from starting when other machines are running and available memory is low.

< Previous Next > Finish Cancel

6. Click **Next** with default Configuration in the **Configure Networking** page.

The screenshot shows a window titled "Create Virtual Machine" with a sub-header "Configure Networking". On the left is a sidebar with a list of steps: "Specify Source", "Specify Name and Location", "Specify Generation", "Assign Processor", "Assign Memory", "Configure Networking" (highlighted in blue), "Connect Virtual Hard Disk", "Installation Options", and "Summary". Above the sidebar is an icon of a server and monitor. The main area contains a text box stating: "Each new virtual machine includes a network adapter. You can configure the the network adapter to use a virtual switch or it can remain disconnected." Below this is a "Connection:" dropdown menu with three options: "VirtualNetwork" (selected), "Not Connected", and "VirtualNetwork". To the right of the dropdown is a "MAC Address" section with a radio button for "Dynamic" (selected) and a radio button for "Static". Below the "Static" option is a text box containing "00 - 00 - 00 - 00 - 00 - 00". Below the "Dynamic" option are two checkboxes: "Enable MAC address spoofing" and "Enable virtual LAN identification". Below these is a "VLAN ID" section with a text box containing "0". At the bottom right are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Create Virtual Machine

Configure Networking

Each new virtual machine includes a network adapter. You can configure the the network adapter to use a virtual switch or it can remain disconnected.

Connection: VirtualNetwork
Not Connected
VirtualNetwork

MAC Address

☒ Dynamic
☐ Static

00 - 00 - 00 - 00 - 00 - 00

☐ Enable MAC address spoofing
☐ Enable virtual LAN identification

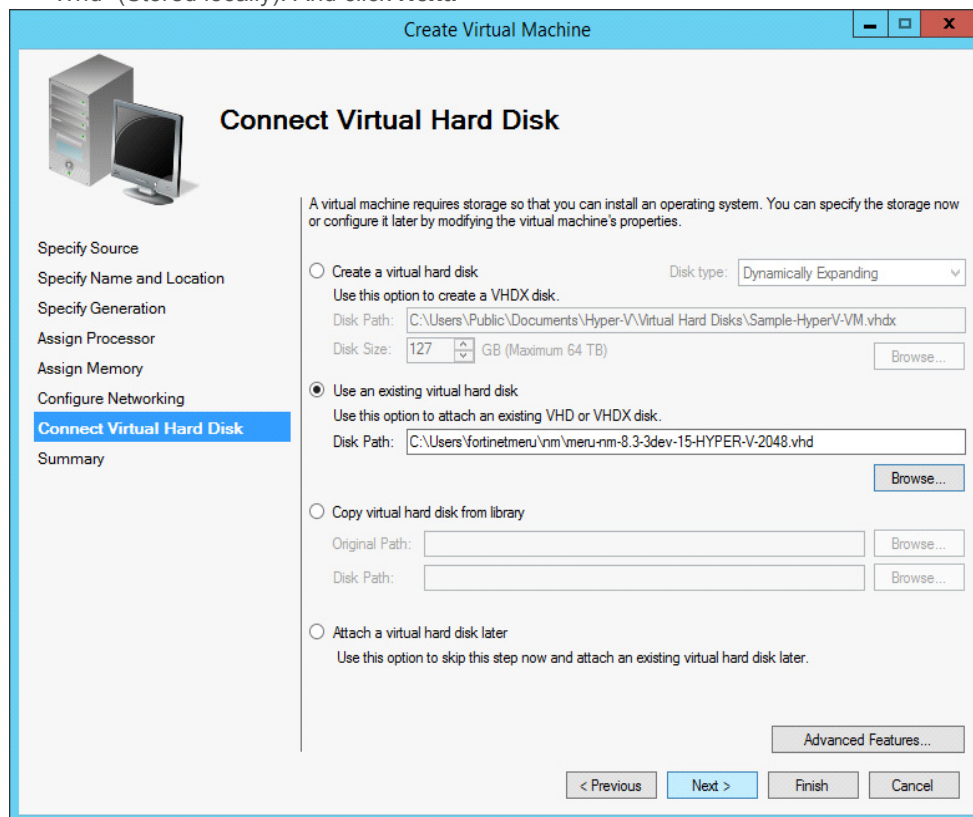
VLAN ID

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

0

< Previous Next > Finish Cancel

7. Select **Use an existing virtual hard disk** and click **Browse** to select the Hyper-V Disk “*.vhd” (Stored locally). And click **Next**.



The screenshot shows the 'Create Virtual Machine' wizard in Windows Server, specifically the 'Connect Virtual Hard Disk' step. The left sidebar contains a list of steps: 'Specify Source', 'Specify Name and Location', 'Specify Generation', 'Assign Processor', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk' (which is highlighted in blue), and 'Summary'. The main area has a title 'Connect Virtual Hard Disk' and a descriptive paragraph: 'A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.' There are four radio button options: 1. 'Create a virtual hard disk' (unselected), with a 'Disk type' dropdown set to 'Dynamically Expanding', a 'Disk Path' field containing 'C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\Sample-HyperV-VM.vhdx', and a 'Disk Size' spinner set to 127 GB. 2. 'Use an existing virtual hard disk' (selected), with a 'Disk Path' field containing 'C:\Users\fortinetmeru\vm\meru-nm-8.3-3dev-15-HYPER-V-2048.vhd'. 3. 'Copy virtual hard disk from library', with 'Original Path' and 'Disk Path' fields. 4. 'Attach a virtual hard disk later', with a note to skip this step and attach later. At the bottom right, there is an 'Advanced Features...' button and a set of navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Create Virtual Machine

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ Create a virtual hard disk
Use this option to create a VHDX disk.
Disk type: Dynamically Expanding
Disk Path: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\Sample-HyperV-VM.vhdx
Disk Size: 127 GB (Maximum 64 TB) Browse...

☒ Use an existing virtual hard disk
Use this option to attach an existing VHD or VHDX disk.
Disk Path: C:\Users\fortinetmeru\vm\meru-nm-8.3-3dev-15-HYPER-V-2048.vhd Browse...

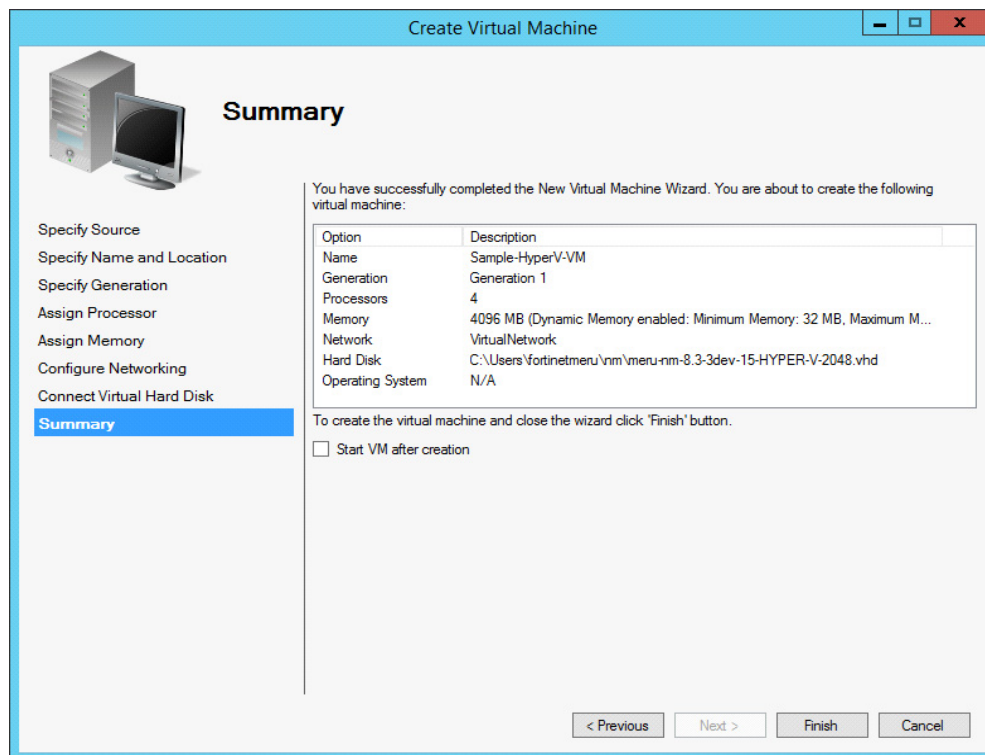
☐ Copy virtual hard disk from library
Original Path: Browse...
Disk Path: Browse...

☐ Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

Advanced Features...

< Previous Next > Finish Cancel

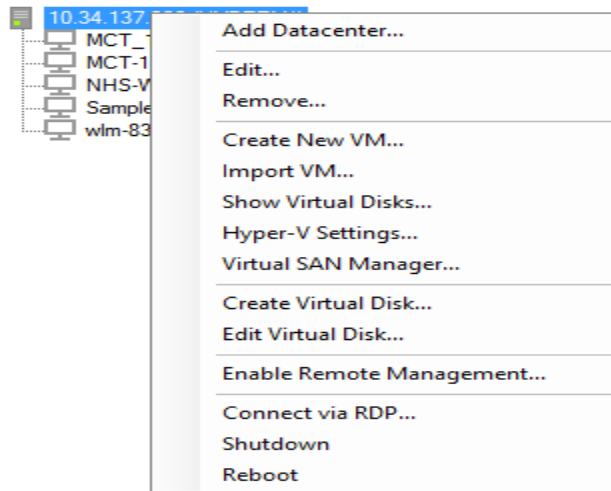
8. Uncheck **Start VM** after creation and click **Finish**.



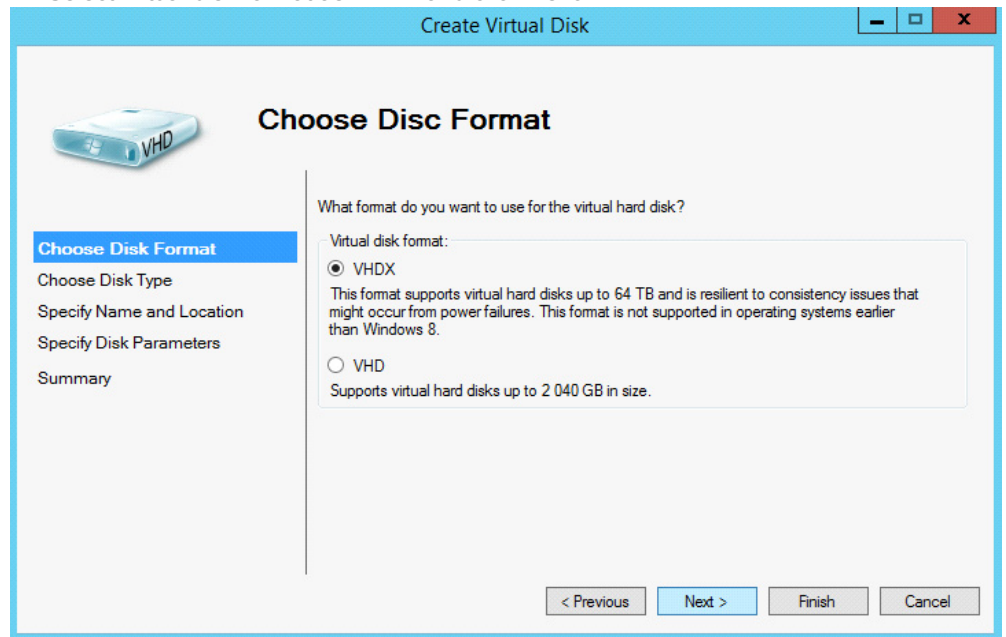
The new Virtual Machine is created.

Creating Virtual Disk

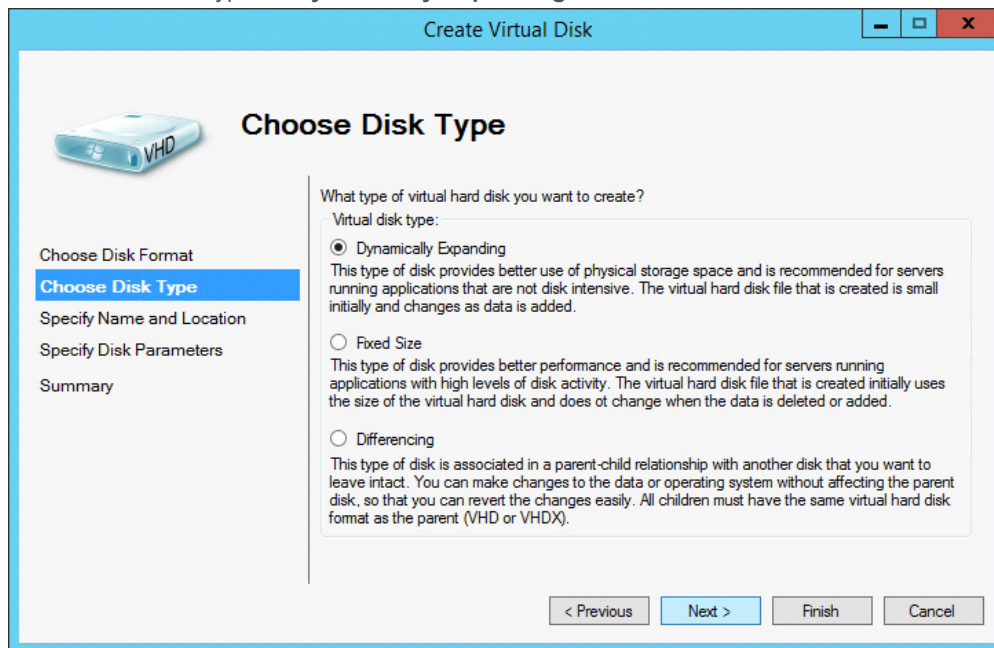
1. Right click on the Hyper-V Server and select **Create Virtual Disk**.



2. Select virtual disk format as **VHDX** and click **Next**.



3. Select the disk type as **Dynamically Expanding** and click **Next**.



The screenshot shows the 'Create Virtual Disk' wizard window. The title bar is blue and contains the text 'Create Virtual Disk' and standard window controls. On the left, there is a sidebar with five steps: 'Choose Disk Format', 'Choose Disk Type' (highlighted in blue), 'Specify Name and Location', 'Specify Disk Parameters', and 'Summary'. Above the sidebar is an icon of a blue hard drive labeled 'VHD'. The main area is titled 'Choose Disk Type' and contains the question 'What type of virtual hard disk you want to create?'. Below this is a section titled 'Virtual disk type:' with three radio button options: 'Dynamically Expanding' (selected), 'Fixed Size', and 'Differencing'. Each option has a descriptive paragraph. At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted in blue), 'Finish', and 'Cancel'.

Create Virtual Disk

Choose Disk Type

Choose Disk Format
Choose Disk Type
Specify Name and Location
Specify Disk Parameters
Summary

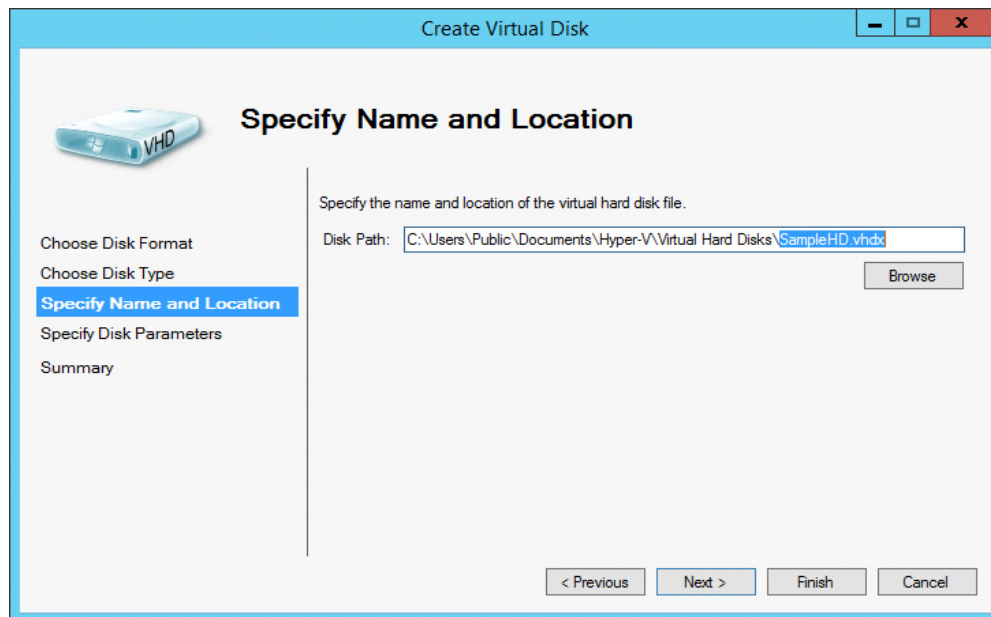
What type of virtual hard disk you want to create?

Virtual disk type:

- ☒ **Dynamically Expanding**
This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.
- ☐ **Fixed Size**
This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when the data is deleted or added.
- ☐ **Differencing**
This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

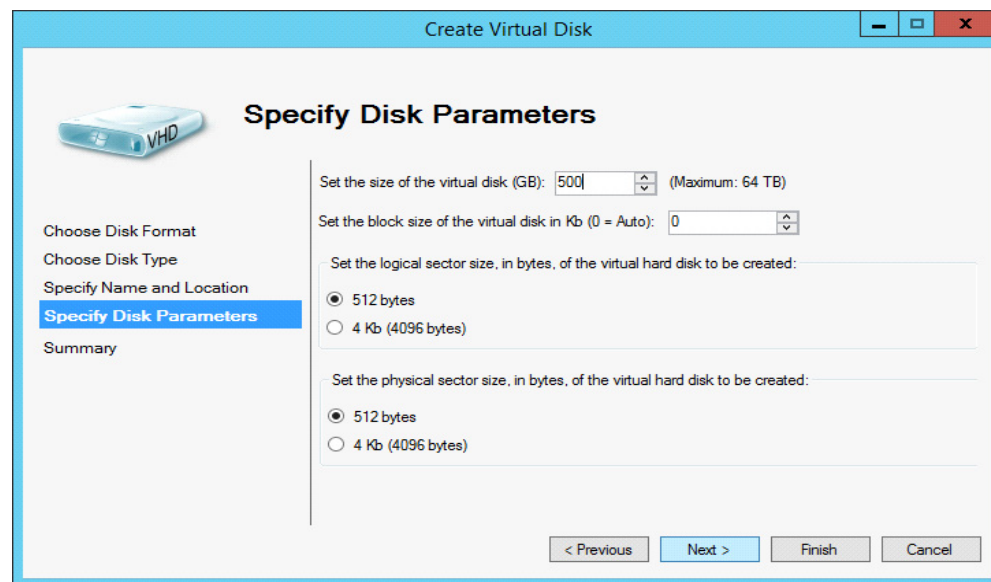
< Previous Next > Finish Cancel

4. Enter the name of the disk and click **Browse** to specify the path to store the virtual disk. Click **Next**.



The screenshot shows the 'Specify Name and Location' step of the 'Create Virtual Disk' wizard. The window title is 'Create Virtual Disk'. On the left, there is a sidebar with a 'VHD' icon and a list of steps: 'Choose Disk Format', 'Choose Disk Type', 'Specify Name and Location' (which is highlighted in blue), 'Specify Disk Parameters', and 'Summary'. The main area has the heading 'Specify Name and Location' and a sub-heading 'Specify the name and location of the virtual hard disk file.'. Below this, there is a 'Disk Path:' label followed by a text box containing 'C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\SampleHD.vhdx'. To the right of the text box is a 'Browse' button. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

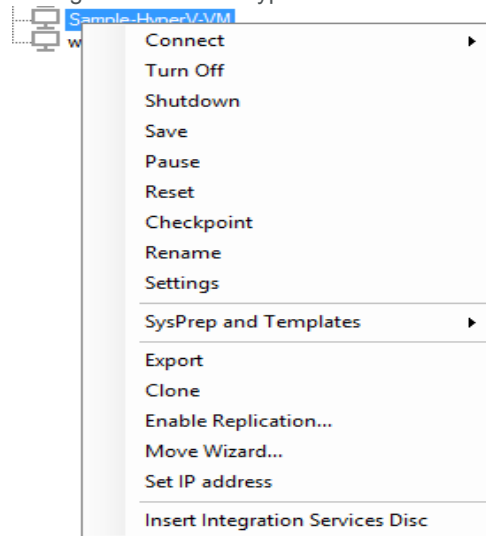
5. Enter the size of the disk. Choose the size of the disk as **500GB / 1TB** and click **Finish**.



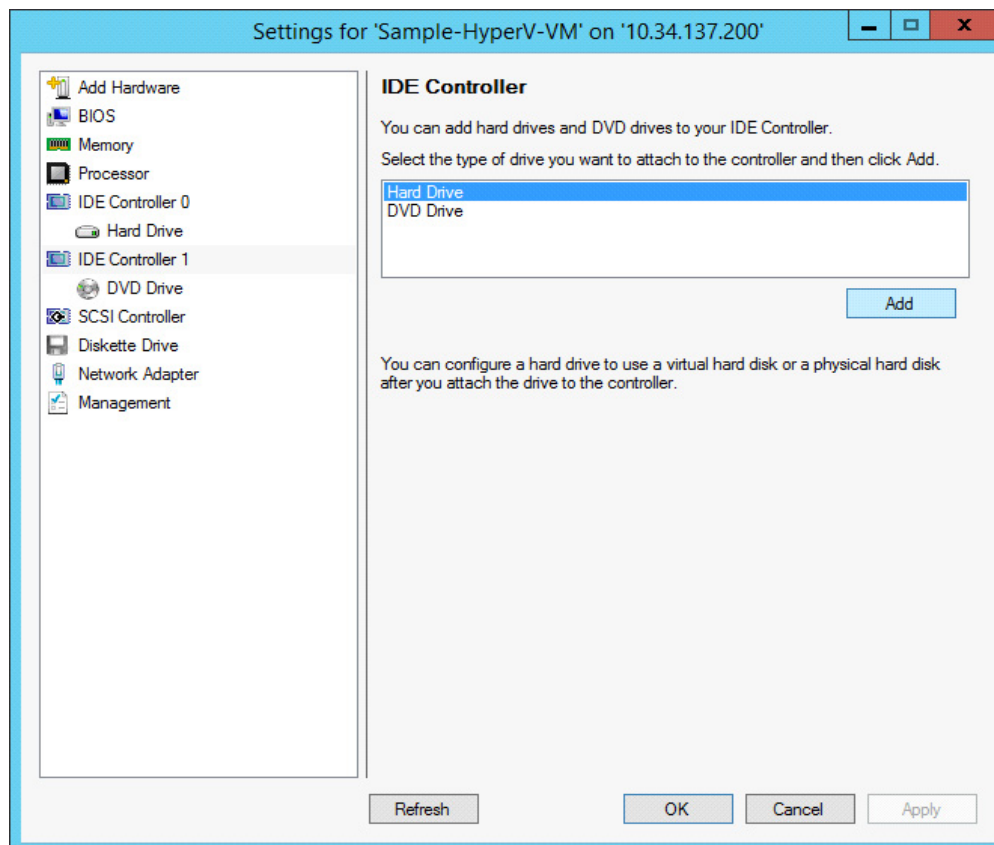
The screenshot shows the 'Specify Disk Parameters' step of the 'Create Virtual Disk' wizard. The window title is 'Create Virtual Disk'. On the left, there is a sidebar with a 'VHD' icon and a list of steps: 'Choose Disk Format', 'Choose Disk Type', 'Specify Name and Location', 'Specify Disk Parameters' (which is highlighted in blue), and 'Summary'. The main area has the heading 'Specify Disk Parameters'. Below this, there are three sections: 'Set the size of the virtual disk (GB):' with a text box containing '500' and a '(Maximum: 64 TB)' label; 'Set the block size of the virtual disk in Kb (0 = Auto):' with a text box containing '0'; and 'Set the logical sector size, in bytes, of the virtual hard disk to be created:' with two radio button options: '512 bytes' (selected) and '4 Kb (4096 bytes)'. Below these, there is another section: 'Set the physical sector size, in bytes, of the virtual hard disk to be created:' with two radio button options: '512 bytes' (selected) and '4 Kb (4096 bytes)'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Post Configuration Settings

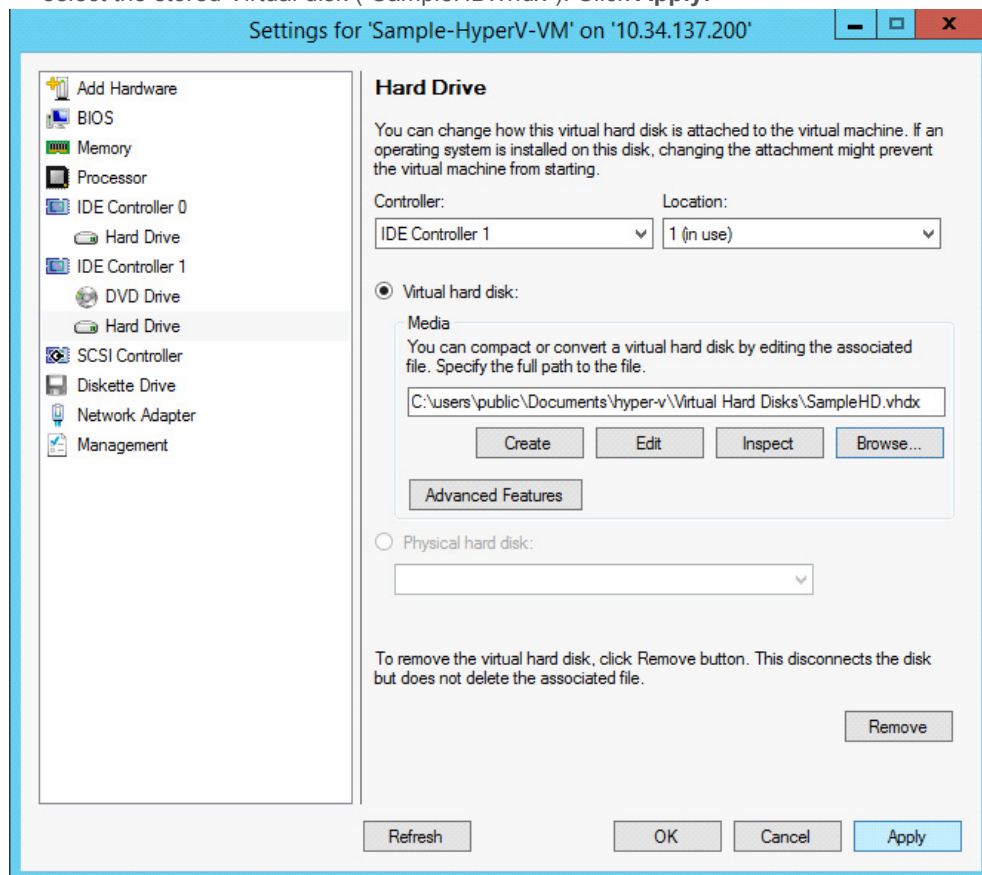
1. Right click on the Hyper-V Virtual Machine and go to **Settings**.



2. Go to **IDE Controller 1**. Select **Hard Drive** and Click **Add**.



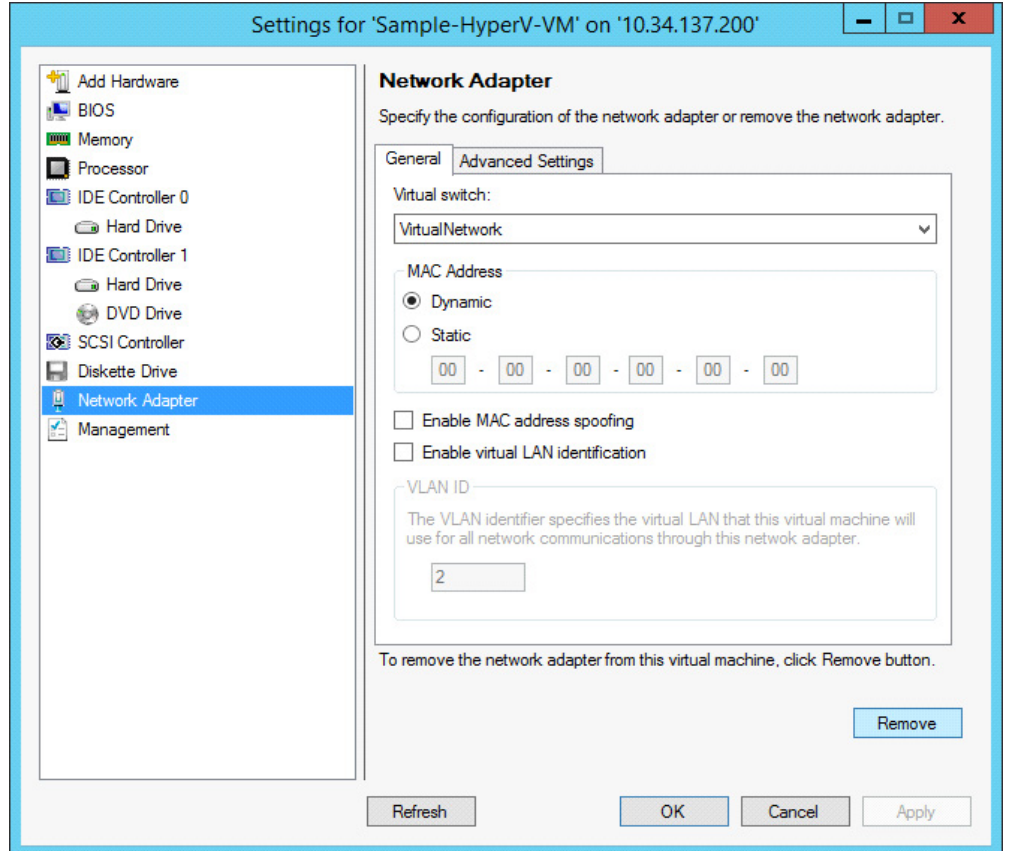
3. Go to newly added hard drive configuration. Select **Virtual hard disk** and click **Browse** to select the stored Virtual disk ("SampleHD.vhdx"). Click **Apply**.



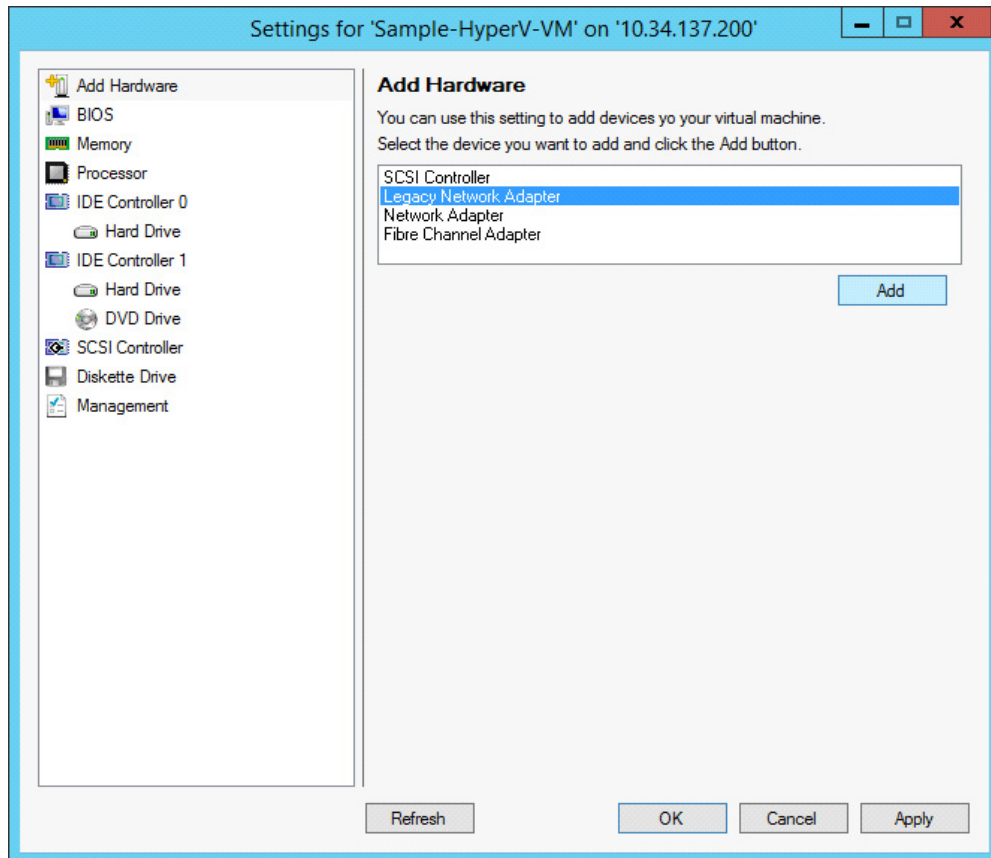
4. Go to **Network Adapter**, click **Remove** to remove the default Network Adapter.

Note:

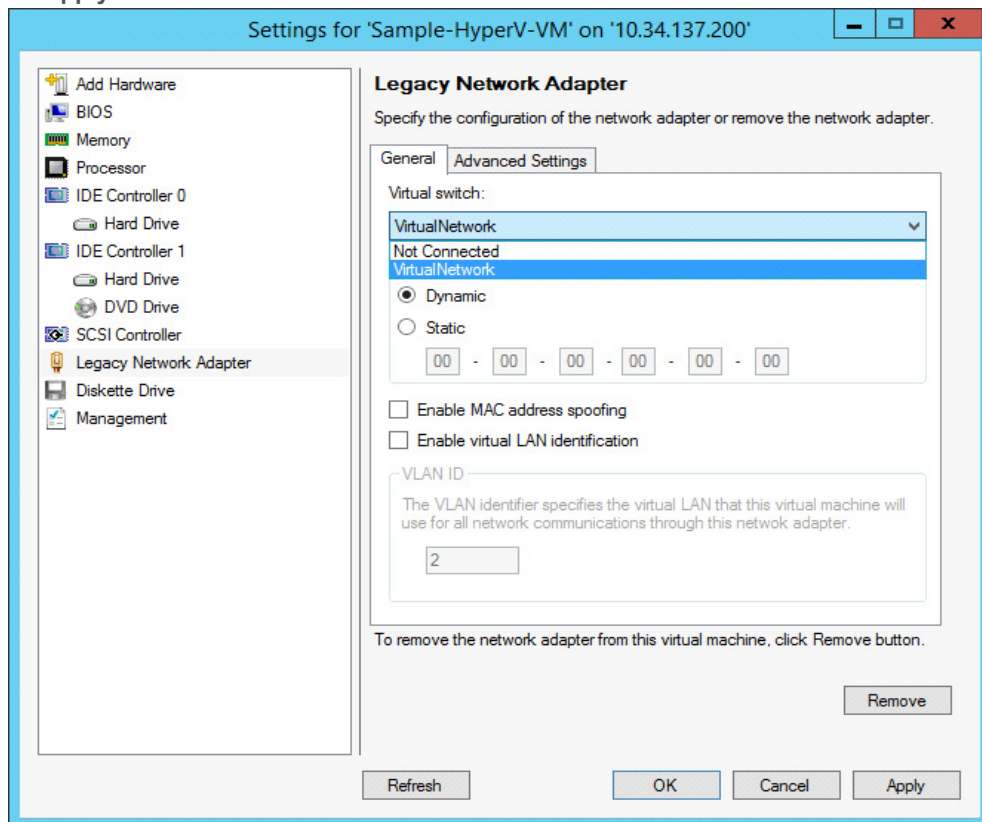
Default Network Adapters are not supported by Hyper-V. Click **Apply**.



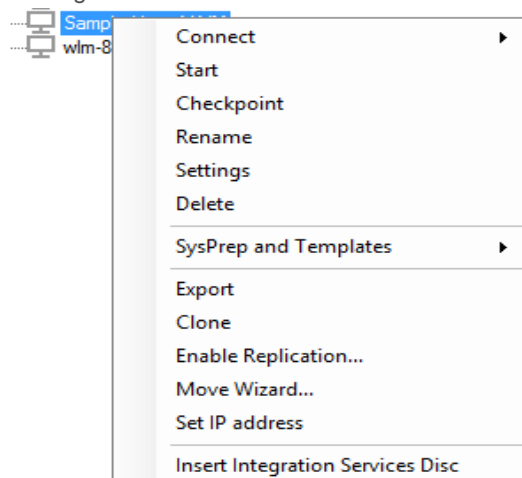
5. Go to **Add Hardware**, select **Legacy Network Adapter** and click **Add**.



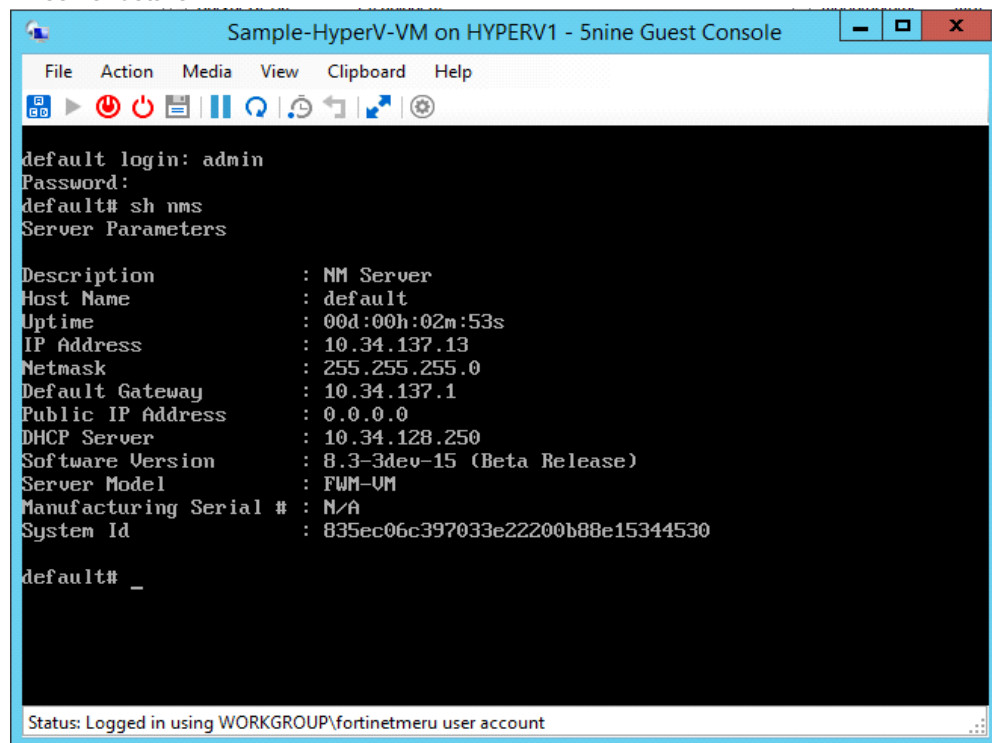
6. Go to **Legacy Network Adapter**, select virtual switch as **Virtual Network** and click **Apply**.



7. Right click on the Virtual Machine and Select **Start** to start the Virtual Machine.



8. When the Virtual Machine is started completely, run the **show nms** command to view the server details.



Deploying FortiWLM with VMWare ESXi 6.5

This document describes the procedure to deploy virtual FortiWLM, **FWM-VM** as FWLM-VM-100D and FWLM-VM-1000D on VMWare ESXi.

Note:

Fortinet recommends VMWare ESXi version 6.5.

Supported Hardware Configuration

This table lists the supported configuration for FWLM-VM-100D and FWLM-VM-1000D.

Configuration	FWLM-VM-100D	FWLM-VM-1000 D
Processor and Cores	Any Processor @ 2GHz or Higher. 4 Cores - 4 Threads	Any Processor @ 3.20GHz or Higher. 4 Cores - 8 Threads
Memory (DRAM)	4GB	16GB
Storage	1TB	2TB
Minimum Disk I/O	100MBps	100MBps
Network	1-4 1G RJ-45	1-4 1G RJ-45
Scale Numbers	AP: 1000 Stations: 5000 Spectrum Sensors: 100	AP: 15000 Stations: 75000 Spectrum Sensors: 750

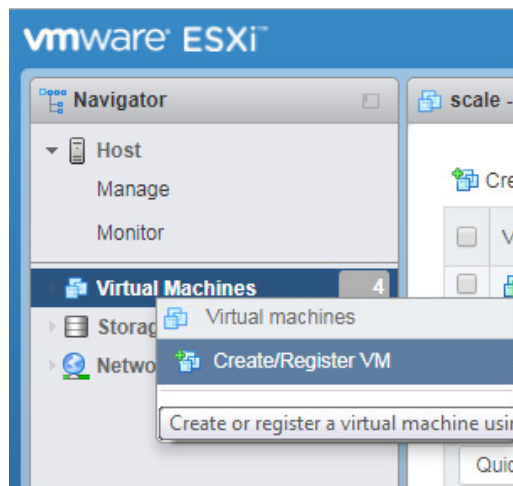
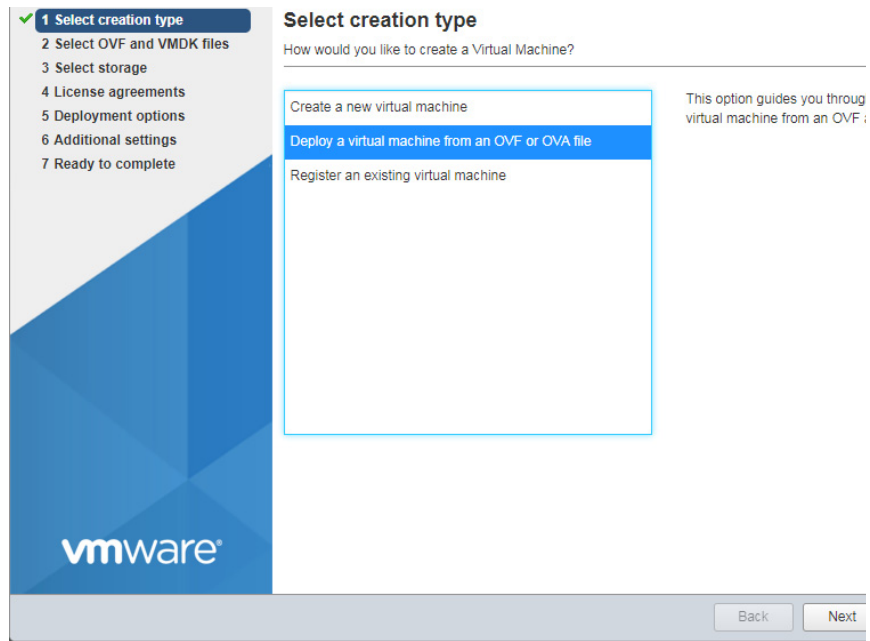
Downloading the Virtual Machine Package File

You can download the virtual controller packages from the Fortinet Customer Support website. To access the support website you need a Fortinet Customer Support account. – **[URL required]**

The file name is, forti-wlm-x.x-xbuild-y-FWM-VM.ova, where x.x-x is the release version number. For example, 8.3.2.

Creating the Virtual Machine

1. Open the VMWare ESXi console and navigate to **Virtual Machines < Create/Register VM**.



The **New Virtual Machine** wizard is displayed.

2. Select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.
3. Enter a unique name for the virtual machine and click on the space, as indicated, to select or drag and drop the downloaded OVA file. Click **Next**.

New virtual machine - FWLM-VM-1000D

✓ 1 Select creation type

2 Select OVF and VMDK files

3 Select storage

4 License agreements

5 Deployment options

6 Additional settings

7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

FWLM-VM-1000D

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi

×

vm

forti-wlm-8.3-2build-5-FWM-VM.ova

Back

Next

4. Select the datastore to store configuration and disk files. Click **Next**.

473

New virtual machine - FWLM-VM-1000D

✓ 1 Select creation type

✓ 2 Select OVF and VMDK files

✓ 3 Select storage

4 License agreements

5 Deployment options

6 Additional settings

7 Ready to complete

vmware

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
Data	15.27 TB	15.15 TB	VMFS6	Supported	Single

1 items

Back

Next

Finish

Cancel

The deployment options are displayed. Click **Next**.

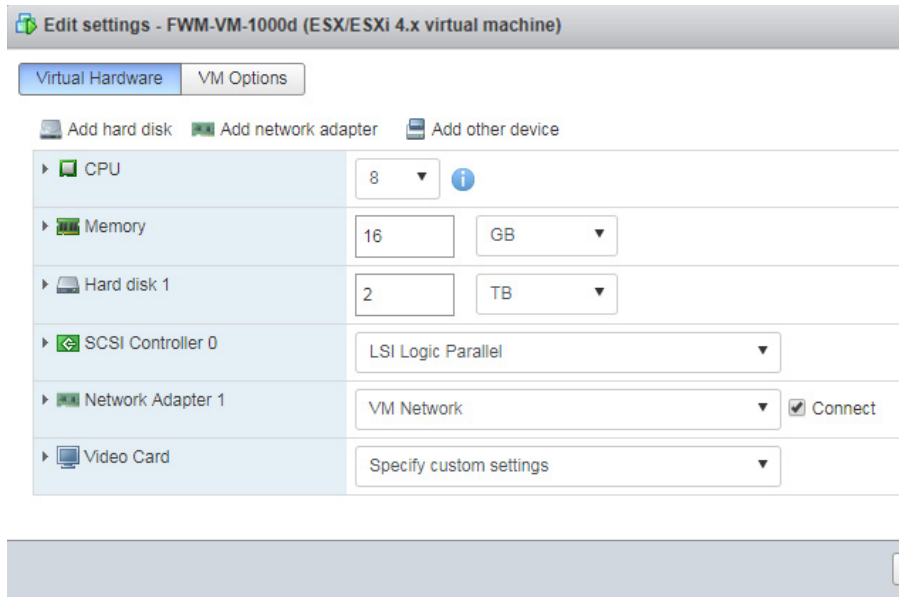
5. Select the **Network mappings** as **bridged VM Network**, **Disk provisioning** should be **Thin**. Disable **Power on automatically**. Click **Next**.
6. Review the configured settings and click **Finish**.

The virtual machine is created.

Configuring the Virtual Machine

After creating a virtual machine, configure it to work as a FWLM-VM-100D or FWLM-VM-1000D.

1. Select the listed virtual machine and right-click. Select **Edit settings**.
2. Modify the **CPU** and the **Memory**. Click **Add hard disk** to add a new hard disk. Click **Save**.



Starting the Virtual Machine

After configuring the newly created virtual machine, select the listed virtual machine and right-click. Select **Power < Power on**.

The Virtual Machine starts.


Expanding the Virtual Hard Disk

You can increase the storage space of a virtual machine by expanding its virtual hard disk. Follow these steps to expand the virtual hard disk.

Note:


Decreasing the size of the virtual hard disk is not supported.


1. Run the **resizedisk** command from the IOS CLI to enable resizing the disk.
2. Select the virtual machine on the ESXi console and right click.
3. Select **Power < Power off** to power off the Guest VM.
4. Right click the virtual machine and select **Edit Settings**.
5. Under **Virtual Hardware**, modify the hard disk size.


 Edit settings - FWM-VM-1000d (ESX/ESXi 4.x virtual machine)








Virtual Hardware

VM Options

 Add hard disk

 Add network adapter

 Add other device

 CPU	8	
 Memory	16	GB
 Hard disk 1	2	TB
 SCSI Controller 0	LSI Logic Parallel	
 Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect
 Video Card	Specify custom settings	

Save

B

Appendix B - Troubleshooting FortiWLM

The following are troubleshooting tips for *FortiWLM*.

#	Problem description	Troubleshooting Tips
1.	How to recover the appliance from the degraded mode	<p>Root cause: Degraded mode indicates that one of the hard disks in the appliance failed.</p> <p>Troubleshooting:</p> <p>Identify the failure hard disk by the RAID status alarm.</p> <p>In CLI use RAID replace <upper/lower> depending on which hard disk has failed.</p> <p>-> Power off nms-server.</p> <p>-> Replace the failure hard disk.</p> <p>-> Power on appliance.</p> <p>After reloading the appliance, the RAID process will restart and the RAID state will be recover mode.</p>
2.	How can I check the details of the appliance like IP address, S/W version details and uptime?	<p>Troubleshooting: You have two options. Log in to the appliance and type the command sh nms in the appliance, or navigate to <i>Administration > System Administration > Server details</i> in the web UI.</p>

#	Problem description	Troubleshooting Tips
3.	<p>Server details are not displayed in the appliance when this command is issued: applianceTesting# sh nms</p> <p>You see the message: <i>Unable to establish communication with configuration server.</i></p>	<p>Root cause: Some of the services might not be started in the appliance.</p> <p>Recover procedure: Reboot the appliance using the command reload nms-server</p>
4.	<p>When loading a new image onto the SA2000, a controller already added to FortiWLM has an upgrade failure.</p>	<p>Root cause: SSH is blocked when a different version of the image is loaded on the FortiWLM SA2000 server.</p> <p>Troubleshooting: Delete the known hosts in FortiWLM SA2000 server and the controller in the path: /root/.ssh/known_hosts</p> <p>Re-add the controller from the web UI.</p> <p>Note: This requires root intervention.</p>
5.	<p>If the administrative state of a controller is inactive, it indicates that discovery is not successful. For example, if you select the controller from inventory and then click Settings, the discovery state is DISCOVERY-STATUS_UP-GRADE_FAILURE.</p>	<p>Root cause: Controller may be in the process of being upgraded.</p> <p>Troubleshooting: Either delete and add the controller or wait and try discovery again.</p>

#	Problem description	Troubleshooting Tips
6.	The discovery state is DISCOVERY_STATUS_IN_PROGRESS .	<p>Root cause: Either the discovery process has hung or the link is too slow.</p> <p>Troubleshooting: Execute the reload nms-server command from IOCLI.</p>
7.	The discovery state is DISCOVERY_STATUS_KEEP_ALIVES_MISSED	<p>Root cause: Either the FortiWLM agent is not running or discovery is not receiving a keep alive message from FortiWLM agent on the controller.</p> <p>Troubleshooting: Verify the status of Agent by executing the command SHOW NMS-SERVER on controller. The result should indicate connected.</p>
8.	The Management server message says UNSUPPORTED_CONTROLLER_VERSION	<p>Root cause: Controller version is not supported by FortiWLM.</p> <p>Troubleshooting: Upgrade the FortiWLM to a compatible software version that supports the System Director.</p>

#	Problem description	Troubleshooting Tips
9.	If the discovery state is “ DISCOVERY_STATUS_CONTROLLER_VERSION_NOT_FOUND ”	<p>Root cause: Discovery process failed to obtain the controller version.</p> <p>Troubleshooting: Verify that you can SSH into the controller and then execute the Show Controller command to make sure that proper values are returned.</p>
10.	If the Management server message displays “agent copy failed”	<p>Root Cause: Image copy failed due to insufficient space on the controller to extract the Image.</p> <p>Troubleshooting: Free up some space on the controller by using delete flash:<older SD version> command.</p>
11.	If the Management state displays “ controller Not reachable ” for VPN Controller	<p>Root Cause: The VPN Controller is upgraded before the running configuration is saved.</p> <p>Troubleshooting: Enter the <i>NMS Server IP</i> and <i>Port Number</i> in the controller to reestablish the VPN [1194] tunnel in the <i>VPN Server Administration</i> screen.</p>

#	Problem description	Troubleshooting Tips
12.	"Authentication Failed"	<p>Root Cause: This message is displayed, if you have entered a wrong password on the controller or if the admin password has been changed.</p> <p>Troubleshooting: Navigate to <i>Inventory > Devices > Controllers > Select a controller > Edit option</i></p> <p>On the <i>Controller Inventory Details</i> screen, in the <i>Password</i> field, update the password and click <i>Save</i> option. The controller is rediscovered.</p>
13.	"Controller Not Reachable"	<p>Root Cause: This message is displayed for the following reasons:</p> <ul style="list-style-type: none"> • The controller is down. • The controller is up and not reachable from E(z)RF server. (It uses port 22). <p>Troubleshooting: Check if port 22 is opened.</p> <p>Once controller is reachable from FortiWLM server, it tries to re-register the controller after 10 minutes.</p> <p>Check the IP Address of the controller. (In case of RMA controller acquires a new IP address).</p>
14.	"Unsupported Controller Version"	<p>Root Cause: This message is displayed, if an unsupported version of controller is connected to the FortiWLM.</p> <p>Troubleshooting: Verify the supported versions of the controller on the <i>FortiWLM</i> by navigating to <i>Administration > System Administration > Supported Controllers</i></p>

#	Problem description	Troubleshooting Tips
15.	<i>"Agent Installation Failed"</i>	Root Cause: <ul style="list-style-type: none"> • Package Security Check Failed. • Integrity Verification Error
16.	"Already added in other server"	Root Cause: The controller is added to different nms-server. Troubleshooting: Controller-cli>>sh nms-server Verify the Server IP/Controller ID/Server connectivity status on the controller. The server IP and controller ID must match with E(z)RF Inventory table. 1 172.18.198.26 3 4.0-6.0-A-16 connected Delete the controller from other E(z)RF server.
17.	"NMS server could not detect controller version"	Root Cause: The controller is not fully operational Troubleshooting: Verify Fortinet services on the controller and restart the service.

#	Problem description	Troubleshooting Tips
18.	"Registration Failed"	<p>Root Cause: This message is displayed during the following possible scenarios:</p> <ul style="list-style-type: none"> • Controller time mismatch • Not enough space <p>Troubleshooting:</p> <ul style="list-style-type: none"> • Verify controller space. • Reset the controller time.
19.	"Controller Time mismatch"	<p>Root Cause: This message is displayed during the following possible scenarios:</p> <ul style="list-style-type: none"> • Controller time mismatch. <p>Troubleshooting:</p> <ul style="list-style-type: none"> • Verify the controller time. • Reset the controller time.
20.	"Installing NMS Agent"	<p>Root Cause: This message is displayed during the following possible scenarios:</p> <ul style="list-style-type: none"> • While installing NMS agent on the controller. • If the E(z)RF server upgrade comprises of more controllers (on a scale setup)

#	Problem description	Troubleshooting Tips
21.	<i>"Heartbeat Missed"</i>	<p>Root Cause: This message is displayed during the following possible scenarios:</p> <ul style="list-style-type: none"> • E(z)RF server misses 3 consecutive "Keep-Alive" message and is not reachable from E(z)RF server. • The controller may be down. <p>Troubleshooting:</p> <p>Verify the link between E(z)RF server and controller.</p>
22.	<i>"Authentication Fail"</i>	<p>Root Cause: The controller "admin" password has been modified on the controller</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> • Navigate to <i>Inventory > Devices > Controllers > Select controller > Edit</i> option. • In the <i>Controller Inventory Details - Update</i> screen, update the controller password in the <i>Password</i> field. • Select Save option. • It triggers controller rediscovery.

C Appendix C - Migrating FortiWLM Data

Migrating from SA200 to SA2000

If you upgrade from an SA200 to the higher capacity SA2000, you can migrate your data to the bigger services appliance. Copy the backup from the external location to the SA2000 and restore the backup. Detailed instructions are given below.

To migrate FortiWLM data from an SA200 to the higher capacity SA2000, follow these steps:

1. Verify available disk space on the production server using the **show file systems** CLI command.
2. If `/data use %` is less than 90%, proceed with production server data backup using the **backup all** CLI command:

```
SA200# backup all
```

```
This command takes time. Do you want to continue [y|n]? y
```

```
SA200# show backup
```

Backup File Name	Size(bytes)
Backup-6.1-30-SA200-2014-12-07-06-37-39.tar.gz	1416915438
Backup-6.1-30-SA200-2014-12-07-01-01-01.tar.gz	1417072953

```
SA200#
```

3. If the `use%` is equal to or more than 90%, free up space by deleting the oldest backup file before proceeding.
4. Make sure the backup was successful using the CLI command **show backup**:

```
SA200# show backup
```

Backup File Name	Size(bytes)
Backup-6.1-30-SA200-2014-12-07-01-01-01.tar.gz	1417072953

Backup-6.1-30-SA200-2014-12-06-01-01-02.tar.gz 1417013311

In the list of backups, the most recent backup is listed first. Check the version (6.1-30 in the example above) and the date (February 7, 2014) to be sure that this is the backup that you want to restore.

5. Copy the backup file from the SA200 appliance to an external location using the CLI command **copy**. For example:

```
SA200# copy /data/backup/nms/Backup-6.1-30-SA200-2014-12-07-06-37-39.tar.gz
ftp://anonymous@<ip address>/
```

6. Turn off SA200 and disconnect it.



It is important that you turn off and disconnect SA200 now because the two services appliance will have the same name after the next step. Failure to turn off SA200 now will result in an IP address conflict between SA2000 and SA200. In addition, the controller can be managed by only one *FortiWLM* services appliance at a time.

7. Set up the SA2000, following the directions in the *Fortinet Services Appliance Guide*. Configure the same host name, network, time zone and other details as those configured on the SA200 server.



It is important that SA2000 have the same name and configuration that SA200 had.

8. Copy the backup file from the external location to the SA2000 using the CLI command **copy**. For example:

```
SA2000# copy ftp://anonymous@<ip address>/Backup-6.1-30-SA200-2014-12-07-
06-37-39.tar.gz /data/backup/nms/
```

```
SA2000# show backup
```

Backup File Name	Size(bytes)
Backup-6.1-30-SA200-2014-12-07-06-37-39.tar.gz	1416915438

SA2000#

Check the version (6.1-30 in the example above) and the date (February 7, 2014) to be sure that this is the backup that you want to restore.

9. Restore the backup on the SA2000 using the CLI command **restore**. For example:

```
SA2000# restore Backup-6.1-30-SA200-2014-12-07-06-37-39.tar.gz
```

This command takes time. Do you want to continue [y|n]? y

SA2000#

10. Verify that the configuration and statistics are restored to the SA2000 server by checking the controller inventory page (**Inventory-> Devices -> Controllers**) to verify all that controller details are restored. Also check the Trend dashboard (**Monitor -> Global Dashboard -> Trend**) to verify that statistics data is restored.



The Migration steps are similar to the above documented procedure of migration from SA200 to SA2000.



The server *Public IP address* that is stored in *Administration > System Administration > Server Details* section is also restored upon initiating the **restore** command.

The *Public IP address* must be modified if it is different from the replaced SA.

D

Appendix D - Resetting System and System Passwords

The passwords for the system users “admin” and “guest” can be reset to their default values during a system boot. When the *FortiWLM* prompts “accepting reset request” display, type **pass** to reset the passwords.

To reset the settings for the entire system to their default values, type **reset** at the reset system values prompt.



By performing a reset of the settings for the entire system, deletes the existing configuration.

Replacing an SA2000 Hard Disk

The SA2000 services appliance uses two disks in a RAID configuration. (SA200 does not have two disks.) If you need to replace one of the hard disks for any reason, follow these steps:

1. From IOSCLI, enter the following command:

raid replace <lower/upper>
2. Power off the SA2000 appliance.
3. Replace the failed hard drive with the initialized replacement drive.
4. Start the SA2000 appliance.

The appliance boots up and the RAID starts in resync mode without any data loss.

E

Appendix E - Command Line Interface

FortiWLM can be accessed from the CLI using the IP address. You must have the access level Admin to use the CLI.

backup

Copies either both the NMS server statistics and configuration or just the configuration to the directory **/data/backup/nm**.

Syntax backup all (NM, SAM, and SM)
backup config-only (NM Config only)

Command Mode Global configuration

Default Full backups are done daily by default.

Usage Log in as *Admin* to do a *data/configuration or a configuration backup*. Backups are written to the directory */data/backup/nms* and have the naming convention Backup-yyyy-mm-dd-hr-mn-sec for *backup all* and Backup_configuration -yyyy-mm-dd-hr-mn-sec for **backup config-only**. By default, two complete backups and all configuration-only backups are saved; you can alter the number of complete backups that are saved.

This table indicates what is copied for a full backup versus a configuration backup:



Backing up requires 5GB of free disk space.

If you use this CLI **backup** command, the web UI backup details will also be updated (*Last Updated, Start Time and End Time columns*) in the GUI history.

There are two possible states for a completed backup: *passed* or *failed*. If a backup or restore fails, error messages are logged into the file `/data/apps/nms/logs/backup.log` and a major alarm is raised for the backup failure. If a backup failed after reaching the maximum hard disk size, the backup entry is listed in the backup history table as failed. Also, a failure message is stored in the log `backup_restore.log`. View this log information using the command **show backup-restore-history** which displays the last 25 entries from the backup-restore-history table.

Example

This command performs a complete backup:

```
default# backup all
```

```
Backup is started. Backup may take several hours depending on system
scale...
```

```
Started compressing backup...
```

```
Successfully backed up the data
```

```
default#
```

The command **show backup** lists the backup file (which includes time and date) and the size of the backup. For example, in this example, backups were done on March 21, 22, 23 of 2013:

```
EzRF1138# sh backup
```

Backup File Name	Size(bytes)
Backup-2013-03-21-01-01-01.tar.gz	376035
Backup-2013-03-22-01-01-01.tar.gz	407017
Backup-2013-03-23-01-01-01.tar.gz	439965

```
EzRF1138#
```

This example uses **delete backup** to delete the backup named Backup-2013-03-05-01-01-01.tar.gz from the directory `/data/backup/nms`:

```
default# delete backup Backup-2013-03-05-01-01-01.tar.gz
```

This command performs a back up of the configuration only:

```
default# backup config-only
```

```
Backup is started. Backup may take several hours depending on system  
scale...
```

```
Started compressing backup...
```

```
Successfully backed up the configuration
```

```
default#
```

Related Command [“restore” on page 515](#)
 [“show” on page 522](#)

calendar

Sets both the hardware clock of the appliance and the time for the NMS server.

Syntax `calendar set <MM/DD/YYYY> <hh:mm:ss>`

Command Mode Global configuration

Default NA

Usage Simultaneously sets both the hardware clock of the appliance and the time for the NMS server; requires a reboot.

Example EzRFserver1148# calendar set ?

 <MM/DD/YYYY> Enter the date in MM/DD/YYYY to set the date.

EzRFserver1148# calendar set 02/21/2013 ?

 <hh:mm:ss> Enter the time in hh:mm:ss to set the clock.

EzRFserver1148# calendar set 02/21/2013 16:13:00

This command requires a controller reboot. Do you want to proceed [yes/no]

y

configure

Sets the admin and/or guest password in the appliance.

Syntax configure terminal

Command Mode Global configuration

Default admin

Usage This command is only used to set the admin and or guest password in the appliance.

Example EzRFserver1148# configure terminal

EzRFserver1148 (config)# ?

end	Exits global configuration mode.
exit	Exits global configuration mode.
passwd	Changes EXEC password.

```
EzRFserver1148 (config)# passwd admin
```

```
<CR>
```

```
EzRFserver1148 (config)# passwd admin
```

```
Changing password for user admin.
```

```
New password:
```

```
BAD PASSWORD: it is too short
```

```
Retype new password:
```

```
passwd: all authentication tokens updated successfully.
```

```
EzRFserver1148(config)#
```

copy

Copies files locally or remotely using either FTP or SCP commands.

Syntax

FTP syntax:

```
copy /data/apps/nms/logs/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz  
ftp://<user name>@<destinationip>/<destination path>
```

SCP syntax:

```
copy /data/apps/nms/logs/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz  
scp://<user name>@<destinationip>/<destination path>
```

FTP syntax to copy a backup file from a remote source to the appliance:

```
copy ftp://<username>@<ipaddress>/Backup-yyyy-mm-dd-hh-mm-ss.tar.gz /  
cddbackup
```

Command Mode

Global configuration

Default

NA

Usage

Copy files to/from the appliance, for example, backup files.

Example

This example gathers diagnostic data on an SA2000 and copies it to another location.

```
EzRF1148# diagnostics
```

```
Getting process information ...
```

```
Getting system log information ...
```

```
Getting kernel information ...
```

```
Getting network information ...
```

```
Getting software information ...
```

```
Getting version information ...
```

```
Getting disk information ...
```

```
Getting Meru data ...
```

Data gathering phase complete

```
/data/apps/nms/logs/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz created
```

Use the copy scp option of the CLI command to move this file off the machine. For example:

```
execute copy /data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz  
scp://<user_name>@<destination_ipaddress><destination_path>
```

```
/data/apps/nms/logs/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz
```

```
EzRF1148# copy /data/apps/nms/logs/meru.gather.EzRF1148.2013-03-23.16-36-  
48.tar.gz scp://<user_name>@<destination_ipaddress><destination_path>
```

Related Command

[“diagnostics” on page 501](#)

crashdump

Command used by Fortinet support to view SA200 logs.

date

Displays today's date and time.

Syntax

date

Command Mode

Global configuration

Default

NA

Usage

Use this command to check the date and time that the appliance is using.

Example

```
default# date
Fri Feb  6 22:13:31 UTC 2013
```

default

Resets some appliance settings to default values.

Syntax

```
default {history | prompt | terminal}
```

history	Restores the history buffer size to the default value (10).
prompt	Restores the prompt string to the default value (host name).
terminal	Sets various terminal characteristics to the defaults.

Command Mode

Global configuration

Default

Usage

Use this command to reset the history buffer, command prompt, and terminal characteristics to default values.

Example

This command resets the history buffer size to 10 commands and then shows the last 10 commands executed on the appliance.

```
default# default history

default# sh history

 3  configure
 4  configure
 5  configure terminal
 6  exit
 7  copy
```

```

8  date
9  debug server
10 debug controller
11 default history
12 sh history

```

delete

Deletes either a file, a backup, or a flash image.

Syntax **delete** {<*filename*> | **backup** <*filename*>| **flash** <*image*>| **app-images** <*image*>}

<i>filename</i>	Name of the file to delete (requires directory information).
<i>backup filename</i>	Deletes named backup file from the directory /data/backup/nms.
flash image	X.X-NNN.
app-images	Deletes the application images.

Command Mode Global configuration

Default

Usage Use this command to delete a backup file or flash image.

Example This example deletes a diagnostics file:

```
default# delete meru.user-diagnostics.EzRF1138.2013-03-03.10-40-03.tar.gz
```

This example deletes a backup image:

```
default# delete backup Backup-2013-03-04-01-01-02.tar.gz
```

This example deletes a flash image:

```
default# delete flash 2.0-141
```


This example deletes a application image:

```
default# delete app-images meru-nms-iphone-feature-1.0-7
```

diagnostics

Gathers NMS server diagnostics into a compressed file.

Syntax **diagnostics**

Command Mode Global configuration

Default NA

Usage Use this command to gather NMS server diagnostics into a compressed file. You can then move the file off of an appliance with either SCP or FTP **copy** commands:

```
copy /data/apps/nms/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz ftp://  
  <user_name>@<destination IP>/<destination path>
```

```
copy /data/apps/nms/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz scp://  
  <user_name>@<destination IP>/<destination path>
```

Example This example gathers diagnostic data on an SA2000 and copies it to another location.

```
EzRF1148# diagnostics  
  
Getting process information ...  
Getting system log information ...  
Getting kernel information ...  
Getting network information ...  
Getting software information ...  
Getting version information ...  
Getting disk information ...  
Getting Meru data ...  
  
Data gathering phase complete
```

```
/data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz created
```

Use the copy scp option of the CLI command to move this file off the machine

```
execute copy /data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz  
scp://<user_name>@<destination IP><destination path>
```

```
/data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz
```

```
EzRF1148# copy /data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-  
48.tar.gz scp://<user_name>@<destination IP><destination path>
```

Related Command

[“copy” on page 497](#)

dir

Displays directory contents.

Syntax

```
dir backup  
dir images  
dir platform-images
```

backup	List the contents of the directory containing backup, /data/backup/nms
images	List the contents of the directory present in the appliance, /opt/meru/images
platform-images	List the contents of the directory containing application images present in the appliance, /data/platform/images

Command Mode

Global configuration

Default

Usage

Use this command to display directory contents.

Example

This example displays the backup directory and then displays the images directory:

```
default# dir ?
```

```
<CR>
```

```
backup                The directory containing the backup databases.
```

```
images                The directory containing the system images.
```

```
default# dir backup
```

```
total 195580
```

```
-rw-r--r-- 1 root root 99023357 Mar 19 01:02 Backup-2013-03-19-13-31-01.tar.gz
```

```
-rw-r--r-- 1 root root 101009548 Mar 19 12:32 Backup-2013-03-20-01-01-01.tar.gz
```

```
-rw-r--r-- 1 root root      1196 Mar 19 12:32 backup_restore.log
```

```
drwxr-xr-x 2 root root    24576 Mar 19 12:32 daily_backup
```

```
default# dir images
```

```
total 136
```

```
drwxrwxr-x 5  522  522  4096 Mar 16 09:14 meru-2.0-156
```

```
drwxrwxr-x 5  522  522  4096 Mar 19 09:14 meru-2.0-157
```

```
-rw-r--r-- 1 root root 23654 Mar 14 11:31 meru.user-diagnostics.default.2013-03-14.11-31-09.tar.gz
```

```
-rw-r--r-- 1 root root 24062 Mar 16 11:03 meru.user-diagnostics.default.2013-03-16.11-03-21.tar.gz
```

```
-rw-r--r-- 1 root root 24902 Mar 18 22:58 meru.user-diagnostics.default.2013-03-19.11-28-02.tar.gz
```

```

-rw-r--r-- 1 root root 23560 Mar 19 11:36 meru.user-
diagnostics.default.2013-03-20.00-06-54.tar.gz

-rw-r--r-- 1 root root 23625 Mar 19 13:25 meru.user-
diagnostics.default.2013-03-20.01-55-51.tar.gz

-rw-r--r-- 1 root root      0 Mar 18 22:57 pre-upgrade-config

-rw-r--r-- 1 root root      0 Mar 20 10:08 script.log

-rw----- 1 root root 1712 Mar 18 22:57 upgrade.log

default#

default# dir platform-images

total 131900

-rwxr--r-- 1 root root 134912139 Dec 29 22:41 meru-4.1.SR1-7-VMC2000.img.gz

drwxr-xr-x 2 522 root      4096 Dec 31 15:40 meru-nms-iphone-feature-1.0-7

drwxr-xr-x 2 522 root      4096 Jan  3 11:30 meru-nms-spectrum-feature-
1.0-9

drwxr-xr-x 2 522 root      4096 Dec 31 17:05 meru-nms-wips-feature-1.0-35

```

enable

Enables privileged mode when you are in non-privileged mode.

Syntax

```
enable <priv mode password>
```

Command Mode

Global configuration

Default

By default, the appliance is already in privileged mode.

Usage

You need to be in privileged mode to enter config mode and use all of the commands. By default, the appliance is already in privileged mode. This command enables privileged mode if you have switched to non-privileged mode. **Enable** works only if you are logged in as admin; guest users cannot switch to privileged mode.

Example

These commands list the options (?) and then switch to privileged mode:

```
EzRF1138> ?

debug                Turns on debugging.
default              Reset to default values.
enable              Enables privileged mode.
exit                Exit the CLI.
help                Displays help information.
no                  Disables various parameters.
prompt              Customizes the CLI prompt.
quit                Exit the CLI.
show                Displays various system parameters.
terminal            Displays or sets terminal characteristics.

EzRF1138> enable *****
EzRF1138#
```

exit

Exit the CLI.

Syntax

exit

Command Mode

Global configuration

Default

NA

Usage

If you exit the CLI, you will have to log in again to execute commands.

Example

```
default# exit
```

help

Displays help information.

Syntax

help

Command Mode

Global configuration

Default

NA

Usage

Use the help command to list all available commands with short descriptions.

Example

default# help

backup	Performs a backup of the nms-server data
calendar	Sets hardware clock and system time but requires a reboot
cd	Sets the current working directory.
certificate	Certificate Management on NM server.
configure	Enter global configuration mode
copy	Copies files locally or remotely
crashdump	Enable or disable crashdump feature, or list crashdumps
date	Displays today's date
default	Reset to default values
delete	Deletes a file from the file system
diagnostics	Gathers FortiWLM diagnostics in a compressed file
dir	Displays directory contents
enable	Enables privileged mode
exit	Exit the CLI
help	Displays help information
no	Disables various parameters
ping	Test network connectivity
poweroff	Power off the system
prompt	Customizes the CLI prompt
pwd	Displays the current working directory
quit	Exit the CLI
raid	RAID management commands
reload	Reboot the nms-server
reload-gui	Restart GUI services
restore	Restores the backed up data
setup	Performs initial setup
show	Displays various system parameters
snapshot	Create or restore a snapshot of the current flash
terminal	Displays or sets terminal characteristics
timezone	Sets the time zone of the system
traceroute	Test network connectivity

no

Disables various parameters such as debug.

Syntax

no <parameter>

ntp-server	Disables time synchronization and removes NTP server settings.
prompt	Disables the display of the CLI prompt.
terminal	Disable the history buffer for the current session.

Command Mode

Global configuration

Default

Usage

Use the **no** command in combination with the three parameters listed above to turn them off.

ping

Tests network connectivity.

Syntax

ping <argument abbreviation>

Argument Abbreviation	Argument	Information
-L	loopback	Suppresses loopback of multicast packets. This flag only applies if the ping destination is a multicast address.
-c	count	Stops after sending count ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.

-i	interval	Waits interval seconds between sending each packet. The default is to wait for one second between each packet normally, or not to wait in flood mode. Only a superuser may set interval to values less than 0.2 seconds.
-w	deadline	Specifies a timeout, in seconds, before ping exits, regardless of how many packets have been sent or received. In this case, ping does not stop after the count packet is sent; it waits either for the deadline to expire, until count probes are answered, or for some error notification from the network.
-p	pattern	You can specify up to 16 pad bytes to fill out a packet you send. This is useful for diagnosing data-dependent problems in a network. For example, -p ff causes a sent packet to be filled with ones.
-s	packet size	Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
-t	ttl	Sets the IP Time to Live.
-l	interface or server.(vlan tag)	Sets the source address to a specified interface address. Argument may be numeric IP address or name of device. When pinging IPv6 link-local address, this option is required.
-M	mtu discovery hint	Selects Path MTU Discovery strategy. The hint may be either do (prohibit fragmentation, even local one), want (do PMTU discovery, fragment locally when packet size is large), or don't (do not set DF flag).
-S	sndbuf	Sets socket sndbuf. If not specified, the default buffers not more than one packet.
-T	time stamp option	Sets special IP timestamp options. Time-stamp option may be either tsonly (only timestamps), tsandaddr (timestamps and addresses) or tsprespec host1 [host2 [host3 [host4]]] (timestamp pre-specified hops).

-Q	tos	Sets Quality of Service -related bits in ICMP datagrams. The tos can be either a decimal or hex number. Traditionally (RFC1349), these have been interpreted as: 0 for reserved (currently being redefined as congestion control), 1-4 for Type of Service and 5-7 for Precedence. Possible settings for Type of Service are: minimal cost: 0x02, reliability: 0x04, throughput: 0x08, low delay: 0x10. Multiple TOS bits should not be set simultaneously. Possible settings for special Precedence range from priority (0x20) to net control (0xe0). You must be root (CAP_NET_ADMIN capability) to use Critical or higher precedence value. You cannot set bit 0x01 (reserved) unless ECN has been enabled in the kernel. In RFC2474, these fields has been redefined as 8-bit Differentiated Services (DS), consisting of: bits 0-1 of separate data (ECN will be used, here), and bits 2-7 of Differentiated Services Code point (DSCP).
	hop1 ...	A hop is an intermediate connection in a string of connections linking two network devices. Each time the packet is forwarded to the next router, a hop occurs.
	destination	Destination is either the IP address or the host name.

[Command Mode	Global configuration
Default	NA
Usage	Use the ping command to test network connectivity.
Example	<pre>default# ping yahoo.com</pre> <pre>PING yahoo.com (206.190.60.37) from 172.18.111.220 : 56(84) bytes of data.</pre>

```
64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=1 ttl=49
time=247 ms

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=2 ttl=49
time=248 ms

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=3 ttl=49
time=249 ms

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=4 ttl=49
time=247 ms
```

poweroff nms-server

Powers off the NMS server gracefully.

Syntax `poweroff nms-server`

Command Mode Global configuration

Default NA

Usage Use the **poweroff nms-server** command to shut down the appliance.

Example

```
EzRF1138# poweroff nms-server

Are you sure you want to poweroff the nms-server [y|n]? y

Broadcast message from root (pts/0) (Tue Mar 24 15:05:37 2013):

The system is going down for system halt NOW!

EzRF1138#
```

Related Command [“reload” on page 514](#)
[“reload-gui” on page 514](#)

prompt

Customizes the CLI prompt.

Syntax `prompt <prompt>`

Command Mode	Global configuration
Default	The default prompt is default .
Usage	Use this command to change the CLI command prompt for the current session only.
Example	<pre>default# prompt ? <prompt> Enter the name of the prompt you want to display. default# prompt MeruDemo MeruDemo#</pre>

pwd

Displays the current working directory.

Syntax	pwd
Command Mode	Global configuration
Default	By default, the path is directed to images in the directory system images.
Usage	
Example	<pre>MeruDemo# pwd images MeruDemo#</pre>

quit

Exits the CLI.

Syntax	<code>quit</code>
Command Mode	Global configuration
Default	NA
Usage	If you execute the command quit , you have to reconnect to the appliance CLI to use it again.
Example	<code>default# quit</code>

raid replace

Use this command on SA2000 only to replace a RAID drive and rebuild the array.

Syntax	<code>raid replace {lower upper}</code>				
	<table> <tr> <td><code>lower</code></td><td>Disengage the lower appliance disk in preparation for removal.</td></tr> <tr> <td><code>upper</code></td><td>Disengage the upper appliance disk in preparation for removal.</td></tr> </table>	<code>lower</code>	Disengage the lower appliance disk in preparation for removal.	<code>upper</code>	Disengage the upper appliance disk in preparation for removal.
<code>lower</code>	Disengage the lower appliance disk in preparation for removal.				
<code>upper</code>	Disengage the upper appliance disk in preparation for removal.				

Command Mode	Global configuration
Default	NA
Usage	<p>Use this command when you need to replace a disk in the RAID array of the appliance. Identify a failed hard disk with the command show raid.</p> <p>if you execute this command on an appliance, it changes the appliance from running mode to degraded mode.</p>



When a RAID array is under reconstruction, rebooting the server may lead to unpredictable result including loss of data.

Example `default# raid replace upper`

reload

Reboots the E(z)RF server (similar to the safe reboot command)

Syntax `reload`

Command Mode Global configuration

Default NA

Usage Use this command to reboot the appliance.

Example `EzRF1138# reload nms-server`

Are you sure you want to reboot [y|n]? y

Broadcast message from root (pts/0) (Tue Mar 24 15:14:51 2013):

The system is going down for reboot NOW!

EzRF1138#

Related Command [“poweroff nms-server” on page 511](#)
[“reload-gui” on page 514](#)

reload-gui

Reloads the Web User Interface.

Syntax `reload-gui`

Command Mode Global configuration

Default	NA
Usage	use this command to recover the appliance from the error system busy . This restarts web service.
Example	default# reload-gui default#
Related Command	“poweroff nms-server” on page 511 “reload” on page 514

restore

The **restore** command restores backups from the directory `/data/backup/nms`. Administrators can restore an entire backup or just the configuration with no statistics (config-only).

Syntax	<code>#restore Backup<build>-<hostname>-<year>-<mm>-<dd>-<hr>-<min>-<sec>.tar.gz</code> <code>#restore Backup_configuration-<build>-<hostname>-<year>-<mm>-<dd>-<hr>-<min>-<sec>.tar.gz</code>
---------------	---

Command Mode	Global Configuration
---------------------	----------------------

Default	All backups are stored in the directory <code>/data/backup/nms</code> .
----------------	---

Usage	The restore backup version of the command restores all data that was backed up (maps, nmsdb, eventdb, reports, controller details, alarms, statistics) when the backup was done with backup all . The restore backup config only version of the command restores only the configuration when the backup was done with backup all . When the backup was done with backup-config-only , the configuration is restored.
--------------	---

Restoring a particular table in the database is not supported. To restore a backup from an external location, use the copy command to copy the file to the appliance, then use the restore command. For example, to copy using ftp:

```
EzRF1138# copy ftp ://<username>@<ipaddress>/Backup-2013-03-04-01-01-02.tar.gz /data/backup/nms/
```

Examples To recover the full backup done December 13th from the backup folder **/data/backup/nms**, use this command:

```
default# restore Backup-2.1-70-SA2000-2013-12-13-01-01-01.tar.gz
```

To recover only the configuration from a backup done December 9th, use this command:

```
default# restore Backup_configuration-2.1-70-SA2000-2013-12-09-18-16-34.tar.gz
```

Related Command [“backup” on page 493](#)
[“copy” on page 497](#)

reload default factory

The **reload default factory** command resets the FortiWLM device to its last known default configuration settings. All other configurations and settings are erased.

Caution:

Fortinet recommends that you take a backup of any data before doing a factory reset. Factory reset will erase all existing data from your device.

Syntax #reload default factory

Command Mode Global Configuration

Default NA

Usage Ensure the following before performing the factory reset:

- Ensure that you have console access to your device.
- Disable HA.

Note:

Configurations that are pushed to controllers, APs and AP Groups are not affected.

Example

```
default# reload default factory
```

```
default#
```

Related Command [“backup” on page 493](#)

“copy” on page 497

setup

Run **setup** for initial services appliance setup, or to add controllers to FortiWLM, or to change the DHCP IP Address to Static.

Syntax

setup

Command Mode

Global configuration

Default

NA

Usage

Run the **setup** command to initialize the appliance for first-time use and to change the following settings after setup: appliance name, NTP server, host name, IP address, DHCP, time, DNS, NTP server settings, admin and guest passwords.

Example

This example sets up the static IP, NAT server, DNS server, and Time zone in the appliance.

```
EzRF1148# setup

Begin system configuration...

Host Name configuration for this machine

Current hostname is EzRF1148

Would you like to change the hostname [yes/no/quit]?: n

Currently default password is used for admin

Would you like to change the password [yes/no/quit]?: y

Changing password for user admin.

New password:

BAD PASSWORD: it is too short

Retype new password:

passwd: all authentication tokens updated successfully.

Currently default password is used for guest
```

Would you like to change the password [yes/no/quit]?: y
Changing password for user guest.
New password:
BAD PASSWORD: it is too short
Retype new password:
passwd: all authentication tokens updated successfully.
IP configuration for this machine.
Would you like to configure networking [yes/no/quit]?: y
Would you like to use Dynamic IP configuration (DHCP) [yes/no/quit]?: n
Please enter the IP configuration for this machine.
Each item should be entered as an IP version 4 style address in dotted-decimal notation (for example, 10.20.30.40)
Enter IP address, or q to quit: 172.18.114.8
Is 172.18.114.8 correct [yes/no/quit]?: y
Enter netmask, or q to quit: 255.255.255.0
Is 255.255.255.0 correct [yes/no/quit]?: y
Enter default gateway (IP), or q to quit: 172.18.114.1
Is 172.18.114.1 correct [yes/no/quit]?: y
Would you like to configure a Domain Name Server [yes/no/quit]?: y
Domain Name Server (DNS) configuration for this machine.
Enter one or more DNS name servers.
For this prompt only use q when finished entering name servers.
Enter Name Server IP Address, or q to quit: 1.1.1.1
Is 1.1.1.1 correct [yes/no/quit]?: y
Enter Name Server IP Address, or q to quit: q
Please enter DNS domain name, or q to quit: fortinet.com

Is fortinet.com correct [yes/no/quit]?: y

The time is now Fri Jun 5 19:03:05 UTC 2013

Would you like to change the time zone for this machine [yes/no/quit]?: y

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) none - I want to specify the time zone using the Posix TZ format.

#? 5

Please select a country.

- | | | |
|---------------------|----------------|-------------------|
| 1) Afghanistan | 11) East Timor | 21) Kazakhstan |
| 31) Myanmar (Burma) | 41) Sri Lanka | |
| 2) Armenia | 12) Georgia | 22) Korea (North) |
| 32) Nepal | 42) Syria | |
| 3) Azerbaijan | 13) Hong Kong | 23) Korea (South) |
| 33) Oman | 43) Taiwan | |
| 4) Bahrain | 14) India | 24) Kuwait |
| 34) Pakistan | 44) Tajikistan | |
| 5) Bangladesh | 15) Indonesia | 25) Kyrgyzstan |
| 35) Palestine | 45) Thailand | |

- | | | |
|------------------|--------------------------|--------------|
| 6) Bhutan | 16) Iran | 26) Laos |
| 36) Philippines | 46) Turkmenistan | |
| 7) Brunei | 17) Iraq | 27) Lebanon |
| 37) Qatar | 47) United Arab Emirates | |
| 8) Cambodia | 18) Israel | 28) Macau |
| 38) Russia | 48) Uzbekistan | |
| 9) China | 19) Japan | 29) Malaysia |
| 39) Saudi Arabia | 49) Vietnam | |
| 10) Cyprus | 20) Jordan | 30) Mongolia |
| 40) Singapore | 50) Yemen | |

#? 14

The following information has been given:

India

The name of the time zone is 'Asia/Calcutta'.

Is the above information OK?

1) Yes

2) No

#? 1

The following command is the alternative way of selecting the same time zone

```
timezone set Asia/Calcutta
```

Set system time for this machine.

Synchronize time with a Network Time Protocol (NTP) server [yes/no/quit]?:
y

Please enter the name or IP address of an NTP server, or q to quit: 1.1.1.1

Is 1.1.1.1 correct [yes/no/quit]?: y

System configuration completed.

```
Do you want to commit your changes and reboot [yes/no/quit]?: y
```

```
Broadcast message from root (pts/0) (Sat Jun 6 00:33:36 2013):
```

```
Now rebooting system...
```

```
The system is going down for reboot NOW!
```



In order to configure NTP Host Name, the user needs to set the DNS Server.

show

Displays various system parameters.

Syntax

show *<parameter>*

arp	Displays ARP table with IP-MAC address mappings
backup	Displays backed up directories
backup-restore-history	Displays the last 25 entries in the backup-restore-history table.
calendar	Displays hardware clock
crashdump	Displays SA200 crash file
debug	Displays the debug information
features	Displays added applications such as Service Assurance Manager
file system	Displays information about the file system
flash	Displays system image filenames in flash memory
history	Displays contents of the history buffer
hostname	Displays host name
memory	Displays memory used by running processes
nms	Displays nms configuration
ntp-server	Displays NTP server used for time synchronization
raid	Displays RAID status
snapshot	Displays the time and date of flash backup created with the command snapshot
terminal	Displays terminal settings
timezones	Displays valid time zone names

Command Mode

Global configuration

Default

NA

Usage

Use this command to display the various information listed above.

Example

This example displays memory used by running processes:

```
default# show memory

MemTotal:      8308116 KB
MemFree:       3179376 KB
Buffers:       173892 KB
Cached:        4687724 KB
SwapCached:    0 KB
Active:        4913624 KB
Inactive:      108524 KB
HighTotal:     7469568 KB
HighFree:      2614564 KB
LowTotal:      838548 KB
LowFree:       564812 KB
SwapTotal:     0 KB
SwapFree:      0 KB
Dirty:         864 KB
Writeback:     0 KB
AnonPages:     59384 KB
Mapped:        148508 KB
Slab:          92120 KB
PageTables:    4740 KB
NFS_Unstable:  0 KB
Bounce:        0 KB
CommitLimit:   4154056 KB
Committed_AS:  583356 KB
VmallocTotal:  118776 KB
```

VmallocUsed: 956 KB

VmallocChunk: 117540 KB

HugePages_Total: 0

HugePages_Free: 0

HugePages_Rsvd: 0

Hugepagesize: 2048 KB

default#

This example lists the last 25 entries in the log backup_restore.log:

EzRF1138# show backup-restore-history

2013-03-18 20-31-46 backup Successfully taken the server backup
in file "Backup-2013-03-18-20-30-08.tar.gz"

2013-03-18 20-32-03 backup Successfully taken the server backup
in file "Backup-2013-03-18-20-31-50.tar.gz"

2013-03-18 20-32-20 delete Deleted the backup file "Backup-2013-
03-18-20-30-08.tar.gz"

2013-03-19 01-01-14 backup Successfully taken the server backup
in file "Backup-2013-03-19-01-01-01.tar.gz"

2013-03-19 12-35-43 restore Restored the server data from the
backup file "Backup-2013-03-18-20-31-50.tar.gz"

2013-03-19 15-54-06 restore Restored the server data from the
backup file "Backup-2013-03-19-01-01-01.tar.gz"

2013-03-20 01-01-01 backup Backup failed. Available disk space is
low!. 7(GB) available from 247(GB) total.

2013-03-21 01-30-39 backup Successfully taken the server backup
in file "Backup-2013-03-21-01-29-28.tar.gz"

2013-03-21 01-30-39 delete Deleted the backup file "Backup-2013-
03-18-20-31-50.tar.gz" on backup limit exceeded

2013-03-21 01-34-21 backup Successfully taken the server backup
in file "Backup-2013-03-21-01-34-09.tar.gz"

2013-03-20 20-09-19 backup Successfully taken the server backup
in file "Backup-2013-03-20-20-09-04.tar.gz"

snapshot

Copies or restores a snapshot of the flash to/from the services appliance disk.

Syntax

snapshot {create | restore | delete}

create	Creates a snapshot of the existing [primary or mirror] partition
restore	Restores the snapshot into the other partition
delete	Deletes the snapshot of the other partition

To **view** all the snapshot execute **show snapshot**

```
EzRFScale# show snapshot
```

```
snapshot.2.1-116.15:17-07-08-2013
```

```
snapshot.2.1-106.01:00-04-18-2013
```

To **delete** the snapshot execute **snapshot delete**

```
EzRFScale# snapshot delete
```

```
snapshot.2.1-106.01:00-04-18-2013
```

```
snapshot.2.1-106.01:00-04-18-2013 deleted.
```

Command Mode

Global configuration

Default

NA

Usage

Use this command for flash backup and recovery to/from the services appliance disk. You can recover primary flash from either mirrored flash or from this backup that you created with snapshot. (Note that the snapshot cannot be copied off of the services appliance.) If you upgrade the services appliance, you cannot use the flash backup snapshot feature. The Snapshot works on SA200, SA250 and SA2000.

Example

This example creates a snapshot:

```
default# snapshot create
```

--- System Snapshot Utility ---

Snapshot function: CREATE

Last snapshot was created: <No valid snapshot exists yet>

Active partition is: /dev/hda2

Source partition is: /dev/hda2

Destination partition is: /dev/hda3

*> The snapshot process disables all system services for up to 20 minutes!
<*

Are you sure you want to proceed? [y/n]

This example restores a snapshot when the primary flash is corrupted:

```
default# snapshot restore snapshot.16:00-04-05-2013
```

You booted from the primary partition.

This command will copy the snapshot image snapshot.16:00-04-05-2013 to the mirror partition.

During snapshot, services will continue to run, but you will not be able to run other commands on this console and system performance will be reduced.

It is recommended to run this command during off-peak hours.

Do you want to proceed? [y/n] y

Copying Data: #####

Operation completed successfully.

tcpdump

Captures the network packets and prints the content to a readable format. It can read packets from a network interface card or from a saved packet capture file.

Syntax

```
tcpdump {-i | -r | -w} <value>
```

- i Specifies the network interface on which the packet capture must be applied. Enter a valid network interface name. For example: eth0, eth1
- r Specifies the saved capture file which needs to be processed by **tcpdump**. Enter the absolute path of captured **pcap/cap** file names.
- w Specifies the path name of the file on which the captured packets must be dumped. Enter a file name file appropriate **cap/pcap** extension.

Command Mode	Global configuration
Default	NA
Usage	This command prints the network traffic with respect to the specified interface and dumps them in to capture files.
Example	<p>This command captures the traffic across the interface eth0 and prints them on the terminal.</p> <pre>default# tcpdump -i eth0 tcpdump: WARNING: eth0: no IPv4 address assigned tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes 06:50:32.332363 IP default.ssh > win7-vparama.fortinet.com.49286: P 1629843522:1629843622(100) ack 2480788854 win 138 06:50:32.332553 IP win7-vparama.fortinet.com.49286 > default.ssh: . ack 100 win 251 06:50:32.332965 IP default.57718 > india-snow.fortinet.com.domain: 15506+ PTR? 41.10.16.172.in-addr.arpa. (43) 06:50:32.333972 IP default.ssh > win7-vparama.fortinet.com.49286: P 100:296(196) ack 1 win 138 06:50:32.334649 IP india-snow.fortinet.com.domain > default.57718: 15506* 1/0/0 (86) 06:50:32.335001 IP default.44653 > india-snow.fortinet.com.domain: 37771+ PTR? 7.0.16.172.in-addr.arpa. (41) This command sets the size of the terminal history buffer:</pre>

This command captures the traffic across the interface eth0 and writes into a pcap file /root/capeth0.pcap

```
default# tcpdump -i eth0 -w /root/capeth0.pcap
```

```
tcpdump: WARNING: eth0: no IPv4 address assigned
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

This command reads the saved capture file /root/capeth0.pcap and prints it in a readable form in the terminal

```
default# tcpdump -r /root/capeth0.pcap
```

```
reading from file /root/capeth0.pcap, link-type EN10MB (Ethernet)
```

```
06:52:53.280228 IP default.ssh > win7-vparama.fortinet.com.49286: P  
1629949234:1629949334(100) ack 2480790470 win 138
```

```
06:52:53.281791 IP default.ssh > win7-vparama.fortinet.com.49286: P  
100:232(132) ack 1 win 138
```

```
06:52:53.281972 IP win7-vparama.fortinet.com.49286 > default.ssh: . ack 100  
win 253
```

```
06:52:53.353649 arp reply 172.18.198.210 is-at 00:90:0b:1a:f0:4f (oui  
Unknown)
```

```
06:52:53.481885 IP win7-vparama.fortinet.com.49286 > default.ssh: . ack 232  
win 252
```

```
06:52:53.780792 arp reply 172.18.198.47 is-at 00:90:0b:28:82:a7 (oui  
Unknown)
```

```
06:52:53.813046 arp reply 172.18.198.200 is-at 00:10:f3:28:70:42 (oui  
Unknown)
```

```
06:52:54.679916 ec:9a:74:c2:a3:62 (oui Unknown) > 09:00:09:09:13:a6 (oui  
Unknown), ethertype Unknown (0x88b7), length 66:
```

```
0x0000:  0040 7f51 000f ec9a 74c2 a360 8648 fd4b  .@.Q....t..`.H.K  
0x0010:  a667 5c83 4176 1df8 7b20 8aca 77f4 5519  .g\Av..{...w.U.  
0x0020:  0800 0900 0302 0000 0000 0000 0000 0000  ....  
0x0030:  a85b b197                                     .[..
```

terminal

Displays or sets terminal characteristics history, length, and width.

Syntax terminal {history | length | width} <value>

history	Displays or sets the size of the terminal history buffer. Enter a value from 0 to 1000.
length	Sets the number of rows for the terminal. Enter a value from 0 to 256.
width	Sets the number of columns for the terminal. Enter a value from 1 to 1024.

Command Mode Global configuration

Default NA

Usage This command changes terminal history, row length or row width if a value is provided and displays the current settings if no value is provided.

Example This command displays the terminal history.

```
default# terminal history
```

- 1 raid
- 2 show memory
- 3 snapshot
- 4 snapshot create

This command sets the size of the terminal history buffer:

```
default# terminal history 25
```

timezone

Sets the time zone of the system.

Syntax

timezone menu

timezone set <zone>

menu	Sets the appliance to a time zone by asking a series of questions
set	Sets the appliance to the time zone named (see list below)

Command Mode

Global configuration

Default

America/Los_Angeles

Usage

Sets the time zone of the system to the specified zone: Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Aruba, America/Asuncion, America/Atikokan, America/Bahia, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Vevay, America/Indiana/Vincennes, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/La_Paz, America/La_Rioja, America/Lima, America/Los_Angeles, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/

Center, America/North_Dakota/New_Salem, America/Panama, America/Pangnirtung,
 America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain,
 America/Porto_Velho, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet,
 America/Recife, America/Regina, America/Rio_Branco, America/Rio_Gallegos, America/
 San_Juan, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/
 Scoresbysund, America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia,
 America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa,
 America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tor-
 tola, America/Tucuman, America/Ushuaia, America/Vancouver, America/Whitehorse,
 America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/
 Davis, Antarctica/DumontDUrville, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/
 Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Vostok, Arc-
 tic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/
 Aqtobe, Asia/Ashgabat, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut,
 Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Choibalsan, Asia/Chongqing, Asia/Colombo,
 Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin,
 Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/
 Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Krasnoyarsk, Asia/
 Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/
 Manila, Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/
 Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon,
 Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/
 Singapore, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Thimphu, Asia/Tokyo,
 Asia/Ulaanbaatar, Asia/Urumqi, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekater-
 inburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/
 Cape_Verde, Atlantic/Faeroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlan-
 tic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/Adelaide, Australia/Bris-
 bane, Australia/Broken_Hill, Australia/Currie, Australia/Darwin, Australia/Hobart, Australia/
 Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/Perth, Australia/Sydney,
 Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belgrade, Europe/Berlin,
 Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Chisinau,
 Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki,
 Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev,
 Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid,
 Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/
 Oslo, Europe/Paris, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/
 San_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/
 Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican,
 Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/
 Zaporozhye, Europe/Zurich, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/
 Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius,
 Indian/Mayotte, Indian/Reunion, Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Eas-
 ter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofu, Pacific/Fiji, Pacific/Funafuti, Pacific/
 Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/

Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis

Example

This example uses menus to set the timezone to Americas > United States > pacific Time. The driveline command is listed at the end of the example.

```
default# Tilimsen menu
```

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) none - I want to specify the time zone using the Posix TZ format.

```
#? 2
```

Please select a country.

- | | | |
|----------------------|-------------------|----------------------|
| 1) Anguilla | 18) Ecuador | 35) Paraguay |
| 2) Antigua & Barbuda | 19) El Salvador | 36) Peru |
| 3) Argentina | 20) French Guiana | 37) Puerto Rico |
| 4) Aruba | 21) Greenland | 38) St Kitts & Nevis |
| 5) Bahamas | 22) Grenada | 39) St Lucia |

- | | | |
|-------------------------|--------------------------|-------------------------|
| 6) Barbados
Miquelon | 23) Guadeloupe | 40) St Pierre & |
| 7) Belize | 24) Guatemala | 41) St Vincent |
| 8) Bolivia | 25) Guyana | 42) Suriname |
| 9) Brazil | 26) Haiti | 43) Trinidad & Tobago |
| 10) Canada | 27) Honduras | 44) Turks & Caicos Is |
| 11) Cayman Islands | 28) Jamaica | 45) United States |
| 12) Chile | 29) Martinique | 46) Uruguay |
| 13) Colombia | 30) Mexico | 47) Venezuela |
| 14) Costa Rica | 31) Montserrat | 48) Virgin Islands (UK) |
| 15) Cuba | 32) Netherlands Antilles | 49) Virgin Islands (US) |
| 16) Dominica | 33) Nicaragua | |
| 17) Dominican Republic | 34) Panama | |

#? 45

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Crawford County
- 7) Eastern Time - Indiana - Starke County
- 8) Eastern Time - Indiana - Switzerland County
- 9) Central Time
- 10) Central Time - Indiana - Daviess, Dubois, Knox, Martin, Perry & Pulaski Counties
- 11) Central Time - Indiana - Pike County

- 12) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
 - 13) Central Time - North Dakota - Oliver County
 - 14) Central Time - North Dakota - Morton County (except Mandan area)
 - 15) Mountain Time
 - 16) Mountain Time - south Idaho & east Oregon
 - 17) Mountain Time - Navajo
 - 18) Mountain Standard Time - Arizona
 - 19) Pacific Time
 - 20) Alaska Time
 - 21) Alaska Time - Alaska panhandle
 - 22) Alaska Time - Alaska panhandle neck
 - 23) Alaska Time - west Alaska
 - 24) Aleutian Islands
 - 25) Hawaii
- #? 19

The following information has been given:

United States

Pacific Time

The name of the time zone is 'America/Los_Angeles'.

Is the above information OK?

Please enter 1 for Yes, or 2 for No.

#? 1

The following command is the alternative way of selecting the same time zone

```
timezone set America/Los_Angeles
```

The time zone is successfully set

```
default#
```

traceroute

Tests network connectivity.

Syntax

```
traceroute <hostname>
```

Hostname refers to any controller or network IP address.

Command Mode

Global configuration

Default

Usage

Check network connectivity with this command.

Example

```
EzRF1138# traceroute 172.18.112.4
```

```
traceroute to 172.18.112.4 (172.18.112.4), 30 hops max, 40 byte packets
```

```
1  172.18.113.1 (172.18.113.1)  1.201 ms  2.049 ms  2.035 ms
```

```
2  172.18.112.4 (172.18.112.4)  1.030 ms  1.039 ms  1.026 ms
```

nms-server unregister (controller command)

Issue this command from a controller to remove or add the controller from/to E(z)RF.

Syntax

```
nms-server unregister  
nms-server register
```

Command Mode	Global configuration
Default	NA
Usage	<p>nms-server unregister unregisters the controller from the server and is only executable from the controller CLI. Once you unregister the controller from the server, the controller goes into an offline inactive state.</p> <p>Once the controller is no longer managed by FortiWLM (nms server), all profiles are owned by the controller and you can edit or delete any profile from the controller, including E(z)RF created profiles. To register a controller, use the command register.</p>
Example	<p>This example unregisters the controller 192.168.143.27 then registers it again. Log on to controller 192.168.143.27 and issue these commands:</p> <pre> EzRF10121 # configure terminal EzRF10121(config)# nms-server unregister 192.168.143.27 SUCCESS: Unregister is complete EzRF10121(config)# example for nms-server register EzRF10121(config)# nms-server register 1 192.168.143.27 34 2.1-3.6.1-A-70 SUCCESS: Register is complete </pre>

upgrade nms-server

Upgrades the appliance to the version indicated.

Syntax	<p>upgrade nms-server <version></p> <p><i>Version</i> will have the format 2.0-159.</p>
---------------	---

Command Mode	Global configuration
Default	NA

Usage

Upgrade the appliance to a new firmware build with this command.

Example

```
EzRF1138# upgrade server 2.0-159
```

```
This will overwrite all existing system images. Are you sure [y|n]? y
```

```
Current Version is 2.0-151
```

```
Upgrading Server
```

```
Stopping Meru services...
```

```
Stopping WLAN services: [#####] Upgrading the  
current configuration. This may take a while. Please be patient ...
```

```
Removing startup database.
```

```
Removing running database.
```

```
Starting upgrade: ##
```

```
Installing base RPMs: #####
```

```
Installing meru-common-2.0-1.i386.rpm: #####
```

```
Installing meru-kernel-2.0-1.i386.rpm: #####
```

```
Installing meru-nms-agent-2.0-1.i386.rpm: ###
```

```
Installing meru-nms-server-2.0-1.i386.rpm: #####
```

```
Installing meru-wnc-2.0-1.i386.rpm: #####
```

```
Installing meru-wnc-key-2.0-1.i386.rpm: ###
```

```
Installing meru-wnc-nms-2.0-1.i386.rpm: #####
```

```
Transition nmsdb to current schema...
```

```
Starting postgresql...OK
```

```
Current nmsdb database version is 2 ...
```

```
Beginning transition to version 3 ...
```

```
Performing upgrade to version 3 ...
```

```
Database transition complete!
```

```
Stopping postgresql...OK
```

Transition eventdb to current schema...
Starting postgresql...OK
eventdb is already up-to-date with version 3.
Stopping postgresql...OK
Upgrade complete.

Broadcast message from root (pts/1) (Tue Mar 24 12:34:32 2013):
Now rebooting system...
The system is going down for reboot NOW!

EzRF1138#

F Appendix E - REST API

FortiWLM exposes the following set of REST APIs that allows you to query the FortiWLM server to get and post the following sub-system information.

Sample Code

You can use the API in your favorite programming language. This document illustrates API calls using PHP code snippets.

NOTE: Fortinet does not provide support for code samples provided in this document.

Fetch Access Token using username and password

```
<?php
$request = new HttpRequest();
$request->setUrl('https://<ip-address>/oauth/token');
$request->setMethod(HTTP_METH_POST);
$request->setHeaders(array(
    'postman-token' => '55e6ca05-bfbb-613f-50c0-5d29562f1ff2',
    'cache-control' => 'no-cache',
    'content-type' => 'multipart/form-data; boundary=---WebKitFormBoundary7MA4YWxkTr-
Zu0gW'
));
$request->setBody('-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="client_id"
ehezoyTLxQN1xb4mxV3dgYA1H2aDruYcZB6gUpwm
-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="client_secret"
uqYymva4V43TLyBXrXS9enHhXSfh4Au5qVIF6MM18CTM4tBpfz
');
```

```

-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="username"
admin
-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="password"
admin
-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="grant_type"
password
-----WebKitFormBoundary7MA4YWxkTrZu0gW--');
try {
    $response = $request->send();
    echo $response->getBody();
} catch (HttpException $ex) {
    echo $ex;
}

```

Fetch Access Token using Refresh Token

```

<?php
$request = new HttpRequest();
$request->setUrl('https://<ip-address>/oauth/token');
$request->setMethod(HTTP_METH_POST);
$request->setHeaders(array(
    'postman-token' => 'e4c9aa40-18b4-eff6-6426-33bf893d4ae5',
    'cache-control' => 'no-cache',
    'content-type' => 'multipart/form-data; boundary=-----WebKitFormBoundary7MA4YWxkTr-
Zu0gW'
));
$request->setBody('-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="client_id"
eheZoyTLxQN1xb4mxV3dgYA1H2aDruYcZB6gUpwm
-----WebKitFormBoundary7MA4YWxkTrZu0gW

```



```

Content-Disposition: form-data; name="client_secret"
uqYymva4V43TLyBXrXS9enHhXSfH4Au5qVIF6MM18CTM4tBpfz
-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="refresh_token"
CDpVS0VIAEFvnQ3ZV54oUn3R5IotjT
-----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="grant_type"
refresh_token
-----WebKitFormBoundary7MA4YWxkTrZu0gW--');
try {
    $response = $request->send();
    echo $response->getBody();
} catch (HttpException $ex) {
    echo $ex;
}

```

Fetching Alarms data using the get API

```

<?php
$request = new HttpRequest();
$request->setUrl('https://10.34.186.228/api/v1.0/alarms');
$request->setMethod(HTTP_METH_GET);

$request->setHeaders(array(
    'postman-token' => 'ebe08df3-e6f2-a8d3-7ac3-b8c6928dea74',
    'cache-control' => 'no-cache',
    'accept' => 'application/json',
    'content-type' => 'application/json',
    'authorization' => 'Bearer I9cbkmmnunbPrj5v9eat6UxyDWGAzcR'
));

try {
    $response = $request->send();
}

```

```

        echo $response->getBody();
    } catch (HttpException $ex) {
        echo $ex;
    }
}

```

AP Groups

Request Type

GET

To get the list of AP groups in your network.

https://<ip-addr>:5000/api/v1.0/apgroups

Input Parameters

None

Response Example

```

{
  "_items": [
    {
      "apGroupType": 1,
      "apGroupId": 2,
      "apGroupName": "10.34.184.134"
    },
    {
      "apGroupType": 1,
      "apGroupId": 4,
      "apGroupName": "10.34.143.27"
    }
  ],
  "_meta": {
    "Status": "Success"
  }
}

```

Request Type

POST

Input Parameters

groupname - Mandatory Parameter

Response Example

```
{
  ""_items"": {},
  ""_meta"": {
    ""Status"": ""Success""
  }
}
```

Syslog / Activities

Request Type GET

To get all the activities in the network. The output can be filtered limit the number entries in the response.

Request URL <https://10.34.184.140/api/v1.0/activities?limit=2>

Response Example

```
{
  "_items": [
    {
      "severity": "info",
      "mnemonic": "Access",
      "timestamp": 1484730623,
      "facility": "security",
      "message": "CLI Session opened for User upgrade from host 10.32.16.29"
    },
    {
      "severity": "info",
      "mnemonic": "Access",
      "timestamp": 1484729318,
      "facility": "security",
      "message": "WEBUI Session logged out from Host 10.32.16.29"
    }
  ],
  "_meta": {
    "Status": "Success"
  }
}
```

Station

Request Type

GET

To get a list of all stations. The response can be filtered to get the entries by matching MAC entries.

`https://10.33.117.100/api/v1.0/station?type=info&mac=04:0c:ce:20:6f:44`

Input Parameters

type - Mandatory

MAC - Mandatory

Request URL

`https://<ip-addr>:5000/api/v1.0/station?type=search&mac=a0`

```
{  "meta": {    "Status": "Success",    "Count": 1  },  "_items": [    {      "timestamp": "1479201460",      "macaddress": "a0:18:28:48:86:a9"    }  ]}
```

Station Log

Request Type

GET

To get station log of a client using its MAC address. Response can be limited using the *Limit* param.

`https://10.33.117.100/api/v1.0/stationlog?mac=04:0c:ce:20:6f:44&limit=2`

Input Parameters

MAC - Mandatory

Response Example

```
{  "_meta": {    "Status": "Success"  },  "_items": [    {      "macaddress": "04:0c:ce:20:6f:44",      "priority": "None",      "details": "<msg_type=ACK><server_ip=10.34.145.200><gateway_ip=10.34.159.1><offered_ip=10.34.159.18>",      "type": "DHCP",      "timestamp": 1484732239,      "logid": 3864,      "controller": "10.34.159.5"    },    {      "macaddress": "04:0c:ce:20:6f:44",
```

```

        "priority": "None",
        "details": "<Old IP discovery Method=none><Old IP=0.0.0><New IP discovery Method=dhcp><New IP=10.34.159.18>",
        "type": "IP Address Discovered",
        "timestamp": 1484732239,
        "logid": 3863,
        "controller": "10.34.159.5"
    }
]
}

```

Access Points

Request Type

GET

To get the list of all access points connected to a controller, identified by its ID.

https://10.34.184.140/api/v1.0/access_points?controllerid=2

Input Parameters

controllerID - Mandatory

Response Example

```

{
  "_items": [
    {
      "apid": 3,
      "runtimecoveryorder": "L3 preferred",
      "uptime": 509274,
      "runtimeversion": "8.3-0build-67",
      "hostname": "10.34.184.134",
      "descr": "AP-3",
      "controllerid": 2,
      "availabilitystatus": "Online",
      "serialnumber": "00:0c:e6:13:15:33",
      "aphwtype": "AP832e"
    },
    {
      "apid": 1,
      "runtimecoveryorder": "L2 preferred",
      "uptime": 0,
      "runtimeversion": "",
      "hostname": "10.34.184.134",
      "descr": "AP-1",
      "controllerid": 2,

```

```

        "availabilitystatus": "Offline",
        "serialnumber": "00:0c:e6:0c:d6:5f",
        "aphwtype": "AP433i"
    }
],
"_meta": {
    "Status": "Success"
}
}

```

Network Summary

Request Type

GET

To get network summary of the FortiWLM server. Some of the items in this response include, alarm count and alarm severity count, number of stations and clients.

<https://10.34.184.140/api/v1.0/nwsummary>

Response Example

```

{
  "_items": [
    {
      "throughput": 0,
      "offlineaps": 1,
      "minoralarms": 0,
      "phones": 0,
      "majoralarms": 0,
      "hostname": "10.34.184.134",
      "stations": 0,
      "onlineaps": 1,
      "criticalalarms": 0
    }
  ],
  "_meta": {
    "Status": "Success"
  }
}

```

Alarms

Request Type

GET

To get list of all alarms from the server.

<https://10.34.184.140/api/v1.0/alarms?limit=2>

Response Example

```
{
  "_items": [
    {
      "severity": "Major",
      "source": "NM",
      "wirelessindex": 0,
      "ifindex": 0,
      "alarm_type": 117,
      "access_point_name": "AP-3",
      "ack_username": "",
      "access_point": 3,
      "fdn": "SD-Rogue-00:0c:e6:14:51:0d",
      "name": "Rogue AP Detected",
      "userack": 0,
      "id": 681,
      "ack_sync_status": 0,
      "acknowledged_at": 0,
      "hostname": "10.34.184.134",
      "raised_at": 1484723756,
      "description": "A NM Rogue AP of MAC address <00:0c:e6:14:51:0d> is detected with APId <3> Channel<36>.",
      "usercomments": "",
      "sequence_number": 0,
      "controller": 2
    },
    {
      "severity": "Major",
      "source": "NM",
      "wirelessindex": 0,
      "ifindex": 0,
      "alarm_type": 117,
      "access_point_name": "AP-3",
      "ack_username": "",
      "access_point": 3,
      "fdn": "SD-Rogue-00:0c:e6:12:f7:99",
      "name": "Rogue AP Detected",
      "userack": 0,
      "id": 677,
      "ack_sync_status": 0,
      "acknowledged_at": 0,
      "hostname": "10.34.184.134",
      "raised_at": 1484723756,

```

```

        "description": "A NM Rogue AP of MAC address <00:0c:e6:12:f7:99> is detected with APId <3> Channel<6>.",
        "usercomments": "",
        "sequence_number": 0,
        "controller": 2
    }
],
"_meta": {
    "Status": "Success"
}
}

```

Request Type PUT

Input Parameters **ack_status** - Mandatory Parameter (can only be 0/1)
alarm_id - Mandatory

Response Example

```

{
    "_items": {},
    "_meta": {
        "Status": "Success"
    }
}

```

Controller AP Inventory

Request Type GET
<https://10.34.184.140/api/v1.0/controllerAPIInventory>

Response Example

```

{
    "_items": [
        {
            "controllerid": 2,
            "np1state": "N+1 Not Configured",
            "hostname": "10.34.184.134",
            "apIds": [
                {
                    "apConnectivityType": "L2 preferred",
                    "apId": 1,
                    "apModel": "AP433i",
                    "apName": "AP-1"
                }
            ]
        }
    ]
}

```



```

    },
    {
      "apConnectivityType": "L3 preferred",
      "apId": 3,
      "apModel": "AP832e",
      "apName": "AP-3"
    }
  ]
},
{
  "controllerid": 4,
  "np1state": "",
  "hostname": "10.34.143.27",
  "apIds": []
}
],
"_meta": {
  "Status": "Success"
}
}
}

```

Controllers

Request Type

GET

To get the list of all controllers connected to the FortiWLM server.

<https://<ip-addr>:5000/api/v1.0/controllers>

Response Example

```

{
  "_meta": {
    "Status": "Success",
    "Count": 2
  },
  "items": [
    {
      "commipaddress": "10.34.186.227",
      "controllerid": 5,
      "hardwaretype": "MC3200",
      "softwareversion": "8.3-0dev-9",
      "descr": "controller",
      "np1state": "N+1 Not Configured",
      "displayaddress": "10.34.186.227",
      "hostname": "10.34.186.227",
      "nodename": "Ctrlr1",
      "nmsstate": "Active",
      "availabilitystatus": "Online",
      "groupid": "default",
      "commipaddress": "10.34.186.226",
      "controllerid": 6,
      "hardwaretype": "MC3200",
      "softwareversion": "8.1-1-9",
      "descr": "controller",
      "np1state": "N+1 Not Configured",
      "displayaddress": "10.34.186.226",
      "hostname": "10.34.186.226",
      "nodename": "Controller",
      "nmsstate": "Active",
      "availabilitystatus": "Online",
      "groupid": "default"
    }
  ]
}

```

Request Type

POST

The following input is sent in the POST message to add a controller.

Input

```

hostname:10.34.12.13
user:sowmya
password:test
port:22

```

connectivity:Use_Default

Response Sample

```
{
  "_meta": {
    "Status": "Success",
    "Count": 1
  },
  "_items": {
    "Message": "10.34.12.13 is controller added "
  }
}
```

Request Type

DELETE

https://10.34.184.149:5000/api/v1.0/controllers/7

Input

hostname:10.34.12.13
user:userone
password:test
port:22

Response Example

```
{  "_meta": {    "Status": "Success",    "Count": 1  },  "_items": [    {      "Message": "Controller deleted Successfully"    }  ]}
```

ESS

Request Type

GET

To get a list of all ESS profiles

https://10.34.186.228/api/v1.0/ess

Response Example{

```
{
  ""_items"": [
    {
      ""fasthandoff"": 0,
      ""essid"": ""ESS2"",
      ""ssid"": ""ESS2"",
      ""mobilitydomain"": 7,
      ""publishessid"": 1,
      ""qamsupport"": 1,
      ""state"": 1
    }, {
      ""fasthandoff"": 0,
```

```

        "essid": "ESS1",
        "ssid": "ESS1",
        "mobilitydomain": 7,
        "publishessid": 1,
        "qamsupport": 1,
        "state": 1
    }
],
"_meta": {
    "Status": "Success"
}
}

```

Input Type	POST <p>To Add an ESS profile</p>
Input Parameters	<p>ESSId - Mandatory Parameter</p> <p>SSID - Optional Parameter (If not given, then the value will be same as EssId)"</p>
Response Example	<pre> { "_meta": { "Status": "Success", "Count": 1 }, "_items": { "Message": "EssTest profile is created " } } </pre>
Input type	DELETE
Input	<p>ESS profile name</p> <p>https://10.34.184.149:5000/api/v1.0/ess/EssTest</p>
Response Example	<pre> { "_meta":{ "Status": "Success", "Count": 1 }, "_items":{ "Message": "EssTest profile is deleted " }} </pre>

Security

Request Type GET
To get the configuration parameters of the default security profile

Response Example

```
https://<ip-addr>:5000/api/v1.0/security
{
  "_meta": {
    "Status": "Success",
    "Count": 1
  },
  "_items": [
    {
      "captiveportalbypassformac": 0,
      "passthroughfirewallfilterid": "",
      "firewallfilterid": "",
      "mfp11wsupport": 0,
      "firewallcapability": 0,
      "l2modesallowed": "Clear",
      "cyphersuites": "None",
      "securityname": "SowmyaSecurity1"
    }
  ]
}
```

Response Type POST
To create or update a security profile

Input

```
Name: sample_security_64len
L2ModesAllowed: WAI PSK/WPI-SMS4
PskKey: ffffffffssssssssccccc
```

Response Example

```
{
  "_meta": {
    "Status": "Success",
    "Count": 1
  },
  "_items": {
    "Message": "sample_security_64len profile is created "
  }
}
```

Wireless

Request Type

GET

Response Example

```
https://<ip-addr>:5000/api/v1.0/wireless
{
  "_meta": {
    "Status": "Success",
    "Count": 1
  },
  "_items": [
    {
      "servicesyncstatus": 1,
      "_ezrf_2authradius_profile": "",
      "_ezrf_1macatradius_profile": "",
      "_ezrf_ess": "sample_ESS1",
      "_ezrf_1accntradius_profile": "",
      "_ezrf_2accntradius_profile": "",
      "backupessid": "",
      "_ezrf_security_profile": "sample_Security1",
      "description": "",
      "_ezrf_hotspot_profile": "",
      "vlansupport": 0,
      "service": "sample_WS1",
      "_ezrf_gre": "",
      "sessiongroupid": "SuperUser",
      "_ezrf_1authradius_profile": "",
      "_ezrf_ess_child": "",
      "backupsecprofile": "",
      "_ezrf_vlan": "",
      "_ezrf_timer_profile": "",
      "_ezrf_vlan_pool": ""
    }
  ]
}
```

Request Type

POST

Input

```
servicename:sample_wirelesspostman
essname:EssTest
```

securityname:SowmyaSecurity1

Response Example

```
{  "_meta": {    "Status": "Success",    "Count": 1  },  "_items": {    "Message": "sowmyawirelesspostman profile is created "  }}
```

Request Type

DELETE

Input

Profile name to be deleted.

https://10.34.184.149:5000/api/v1.0/wireless/sowmyawirelesspostman

Reponse Example

```
{  "_meta": {    "Status": "Success",    "Count": 1  },  "_items": {    "Message": "sowmyawirelesspostman is wireless profile deleted "  }}
}
```

OAuth

Input Type

POST

https://10.34.186.228/oauth/token

Response Example

```
"{  ""access_token"": ""4iRl99mc6oWev0FAyDQupto0VjwG17"",  ""token_type"": ""Bearer"",  ""refresh_token"": ""sbaWq2GRcu6hgXgZmmHfLYW4x1yi6d"",  ""scope"": ""superadmin admin tenant shop""
}"
```

G

Appendix F - WLAN Security Sensors capability

The *Hardware Sensors (AP433is/PSM3x) Spectrum Manager* is an RISC based subsystem in a sensor. It is completely dedicated to monitor the airwaves of the time. By having a dedicated subsystem, the sensor is able to classify and report on the type and source of interference almost instantly and without taking CPU resources away from the wireless radio.

Fortinet WLAN is designed to work with one available channel and still provides a better user experience over systems requiring multiple available channels. The other systems may change the channel of Access Points to avoid potential interference. This often leads to a worse degradation of the overall performance of the network, as the underlying systems are not designed to cope with many number of Access Points sharing the same channel.

With Fortinet, the complete network or a part of the network can be moved to a clearer channel. Fortinet's Air Traffic Control partitions the wireless airspace and delivers high quality connections to the wireless users.

Fortinet sensors capability

- Analog cordless phones
- Frequency- Hopping Spread Spectrum (FHSS) digital cordless phones
- Direct-Sequence Spread Spectrum (DSSS) digital cordless phones
- Motorola Canopy Wireless
- Non-Wifi Wireless Bridges
- Wireless video cameras
- Wireless game controllers
- Conventional microwave ovens
- Inverter microwave ovens
- Motion Detectors (S-Band radar-based)1-4 second typical classification time
- Wireless baby monitors
- Estimates channel utilization for both 802.11 and non-802.11 traffic

Spectrum Manager Radio

- Embedded classification processor with dedicated memory

- 40MHz analysis bandwidth
- 80MHz sampling frequency
- Concurrent 2.4GHz and 5GHz WLAN frequency band sampling
- -90 dBm to 0dBm detection range
- Frequency bands. 2.4GHz to 2.5GHz and 4.9GHz to 5.875 GHz

IEEE 802.11Radio

- Frequency Band
2.402 to 2.485 GHz, 5.15 to 5.25 GHz, 5.725 to 5.825 GHz
- Operating Channels
1 through 11 for 2.4 GHz band
32 through 160 for 5 GHz band
- Data Rates (Mbps)
20 MHz: 130, 117, 104, 78, 65, 58.5, 54, 52, 48, 39, 36, 26, 24, 19.5, 18, 13, 12, 11, 9, 6.5, 5.5, 2, 1 Mbps
40 MHz: 300, 270, 243, 216, 162, 135, 121.5, 108, 81.5, 81, 54, 48, 40.5, 36, 27.5, 27, 24, 18, 13.5, 12, 11, 9, 6, 5.5, 2, 1 Mbps with automatic rate adaption
- Average Transmit Power
2.4n (20 HT): 17 dBm, 2.4n (40 HT): 16 dBm
5.0n (20 HT): 18 dBm, 5.0n (40 HT): 16 dBm
- Receive Sensitivity (for max data rates)
11a: -77 dBm, 11n (5 GHz): -72 dBm, 11g: -77 dBm,
11n (2.4 GHz): -74 dBm



For **PSM3x** sensor AP, the **IEEE 802.11Radio** cannot be used for service clients. It can be used for *WIPS*, *SAM* and *Location* tracking and so on.
In **AP433is** sensor AP, the **IEEE 802.11Radio** can be used for service clients.

For further information, refer to the SAM and WIPS *User Guide*.